



INTERNATIONAL CIVIL AVIATION ORGANIZATION



ICAO Crisis Management Framework Document (EUR Doc 031)

-Second Edition-

2023

TABLE OF CONTENTS

CHAPTER 1. INTRODUCTION	1
1.1 BACKGROUND.....	1
1.2 SCOPE AND OBJECTIVES	3
1.3 DOCUMENT MAINTENANCE	3
CHAPTER 2. DEFINITIONS & ACRONYMS	4
CHAPTER 3. RISK MANAGEMENT	6
3.1 RISK REGISTER	6
3.2 RISK ASSESSMENT	6
3.3 RISK MITIGATION	6
3.4 RISK ACCEPTANCE CRITERIA.....	7
3.5 MITIGATION STRATEGIES.....	8
3.6 MITIGATION CONTROLS.....	8
CHAPTER 4. RESILIENCE, CONTINGENCY, AND CRISIS	10
4.1 OBJECTIVE	10
4.2 EVENT LIFE CYCLE	10
4.3 CRISIS MANAGEMENT PLAN	11
4.4 CONTINGENCY PLAN	11
4.5 EVALUATION AND “LESSONS LEARNT”	12
4.6 NON-EVENT RELATED ACTIVITIES	13
CHAPTER 5. IMPLEMENTATION ASPECTS	14
5.1 INTRODUCTION	14
5.2 TRAINING.....	14
5.3 EXERCISES	14
5.4 ROLES & RESPONSIBILITIES	15
5.5 COMMUNICATION	15
CHAPTER 6. NATIONAL CRISIS MANAGEMENT STRUCTURES	18
6.1 GENERAL	18
6.2 NATIONAL STRUCTURES.....	18
CHAPTER 7. REGIONAL COORDINATION.....	19
7.1 REGIONAL STRUCTURES	19
CHAPTER 8. INTERNATIONAL COOPERATION.....	20
8.1 STRUCTURES	20
8.2 ORGANISATIONS	20
CHAPTER 9. SCENARIO CATEGORIES	21
9.1 INTERNAL	21
9.2 EXTERNAL	21

APPENDIX A – SCENARIOS	24
1 CRI-001 – FLOODS	25
2 CRI-002 – EARTHQUAKE	27
3 CRI-003 – VOLCANIC ASH	29
4 CRI-004 – NUCLEAR INCIDENT	31
5 CRI-005 – ARMED CONFLICT	33
6 CRI-006 – DANGEROUS CHEMICAL INCIDENT	35
7 CRI-007 – FIRE.....	37
8 CRI-008 – SECURITY INCIDENT	39
9 CRI-009 – AIRBORNE SPREAD OF DISEASES-PANDEMIC.....	41
10 CRI-010 – MAJOR FAILURE OF PAN-EUROPEAN FUNCTION.....	43
11 CRI-011 – INDUSTRIAL ACTIONS.....	45
12 CRI-012 – CYBER ATTACK.....	47
13 CRI-013 – SEVERE METEO SITUATION	49
14 CRI-014 – SPACE DEBRIS & METEORITES	51
15 CRI-015 – SPACE WEATHER.....	53
16 CRI-016 – SHORTAGE OF FUEL.....	55
17 CRI-017 – LARGE SCALE POWER OUTAGE	57
18 CRI-018 – LARGE SCALE COMMUNICATION NETWORK OUTAGE	59
APPENDIX B – SCENARIO SCOPE	61
APPENDIX C – SCENARIO RELATIONSHIPS.....	62
APPENDIX D – RISK REGISTER EXAMPLE	63

RECORD OF AMENDMENTS

Amdt. Number	Effective Date	Details
2nd Ed.	January 2024	Approved by EASPG Conclusion 5/XX This new edition comprises a comprehensive change to the document.

ICAO CRISIS MANAGEMENT FRAMEWORK

CHAPTER 1. INTRODUCTION

1.1 BACKGROUND

- 1.1.1 As a consequence from the volcanic eruption in Iceland in 2010, the ICAO 12th Air Navigation Conference (AN-Conf/12) in Montréal in 2012 issued recommendation 4/8 “Crisis Coordination Arrangements and Contingency Plans” stating that ICAO should consider how crisis coordination arrangements for potentially disruptive events, including those events that may adversely impact aviation safety could be established on a regional basis.
- 1.1.2 The European Air Navigation Planning Group (EANPG) initiated the establishment of a standardised framework/concept for the management of crisis situations affecting aviation within the EUR Region, regardless of the type of crisis. This framework/concept included crisis coordination arrangements (i.e. the comprehensive framework for crisis management that had been established in the context of the EU Single European Sky policy through the European Aviation Crisis Coordination Cell (EACCC) supported by the Network Manager, based on EC Regulation 677/2011) and crisis management principles, a non-exhaustive list of possible threat types, the four different phases of crisis escalation and the requirement for pan/intra-regional coordination. The framework/concept was published as EUR Doc 031 in 2014 and has been used as complimentary guidance material to the existing ICAO provisions (e.g. ICAO Annex 11 on contingency arrangements).
- 1.1.3 Whereas the management of the impact of the eruption of the Icelandic volcano in 2010 required a common approach at European level for a few weeks, the management of the impact of the COVID-19 crisis on aviation required continuous efforts at global, regional and national levels for more than two years.
- 1.1.4 During the ICAO EUR/NAT-Directors General of Civil Aviation (DGCA) meeting in September 2021 the lessons learnt from the past and current crisis affecting the civil aviation system were discussed and with respect to the regional aviation crisis preparedness and response mechanisms, the DGCA meeting agreed on the following conclusions:
- a) Close cooperation between European authorities, States and aviation industry is instrumental for any arrangements designed to manage and overcome crisis events with a negative impact on air transportation.
 - b) Considering the international nature of civil aviation, there is a need for efficient regional cooperation mechanisms to tackle major events affecting air transportation regardless their source (safety, security, health etc.) at technical and political level.
 - c) Systematic and efficient coordination of all involved national stakeholders, including public health, through National Air Transport Facilitation Committees is key for, preparedness and crisis response at the national level.
 - d) Taking under consideration the existing ICAO SARPS, PANS and newly developed guidance for the COVID -19 pandemic, enhance compliance with the ICAO provisions and coordination through existing mechanisms (e.g. CAPSCA, VACP, crisis coordination teams) to facilitate improved preparedness planning and crisis management for future events impacting aviation.
 - e) The past crisis events demonstrated that only Pan-European solutions compliant with ICAO SARPS and guidelines can be effective in providing solutions as it was achieved for the adoption of the EASA - ECDC COVID-19 Aviation Health Safety Protocol. Isolated and uncoordinated actions to an event of international nature should be avoided. The EUR aviation crisis

management framework, associated mechanisms such as the European Aviation Coordination Crisis Cell and currently existing guidance material (e.g. EUR DOC 031) need to evolve in order to better manage events affecting aviation and not only network crises.

- f) States need to cooperate closely based on pre-defined arrangements taking into consideration safety, security and other aspects and necessity to ensure a quick recovery for the primary benefit of passengers and the aviation industry. Regional contingency and coordination plans and preparedness exercises are essential in that regard.
- g) Notwithstanding operational or financial impact on industry and on passengers' experience, safety, security and other aspects of any crisis need to be considered as a key element of a response to an event.
- h) Information sharing on safety, security and other risks and risk mitigation measures between States and industry is a key element to ensure readiness for a crisis. States and industry players should actively engage in the existing or yet to be established regional mechanisms for information sharing.
- i) Recognizing benefits resulting from the existing coordination mechanisms at European level, a further reflection should be sought how to ensure more agility and coordination in the future, including inter-sectoral cooperation. To this end, it is proposed that ICAO, EASA, EUROCONTROL Network Manager, States and stakeholders such as ACI, CANSO and IATA coordinate and propose further improvement proposals to the EUR crisis management framework for the DGCA consideration.

1.1.5 A High-level Conference on COVID-19 (HLCC 2021) was held in October 2021 and reached a global consensus on the safe and efficient recovery of aviation from the COVID-19 crisis. During the conference not only the safety, economical and facilitation objectives were addressed, it was also an opportunity to promote and strengthen collective efforts to harmonize measures and risk management strategy through the implementation of the recommendations by the ICAO Council Aviation Recovery Taskforce (CART). In the ministerial declaration it was noted that ICAO is well positioned to support the long-term resilience of international aviation and incorporate the lessons learned from the current and past pandemics, by enhancing its crisis response capability, and regularly reviewing and updating ICAO's Standards and Recommended Practices and guidance materials as may be required.

1.1.6 A Project Team was established in May 2022 which was tasked to review/update the ICAO EUR Doc 031 and especially to include risk management at global/regional/national levels and to refine the existing guidance for crisis management (including elements such as a register of appropriate risks and their assessment, crisis preparedness activities, crisis management procedures and exercises).

1.1.7 As an outcome of the 41st ICAO Assembly in October 2022, the Resolution A41-11 (Declaration on air transport facilitation affirming global commitment to enable the safe and efficient recovery of aviation from the COVID-19 pandemic, and to make aviation more resilient in the future) highlighted the importance of an effective crisis response framework for future public health-related crises that draws on relevant guidance, best practices, integrated risk management approaches, and lessons learned from the COVID-19 pandemic to enable the international aviation community to rapidly respond to a public health-related crisis; and building resilience to future similar outbreaks.

1.1.8 The Strategy on disaster risk reduction and response mechanism in aviation was addressed in Resolution A41-13 which advocates for the evolution of the current global crisis management framework towards a multilayer crisis management approach to support a predictable and harmonized operational response to crisis.

1.1.9 The importance for strengthening the aviation industry to future crisis was also included into the Assembly Resolution A41-24 (Aviation's contribution towards the United Nations 2030 Agenda for

Sustainable Development) in which States are encouraged to enhance the resilience of their aviation systems through including crisis preparedness plans and risk management measures in their aviation policies, planning and operations in order help to maintain essential mobility for air passenger and the transport of critical goods in the face of crises while ensuring the safety of the aviation workforce.

1.2 SCOPE AND OBJECTIVES

- 1.2.1 The *Air Transportation System* is a large and complex system with a lot of interfaces and dependencies. This open nature makes it susceptible for external disturbances. It is, therefore, essential that a clear and comprehensive overview of risks and possible mitigations for the air transportation system disrupting events is made.
- 1.2.2 This document contains the definitions and explanation of the terms pertinent to the air transportation system disruptions and provides regional guidance material for increasing the resilience of the system in the ICAO EUR Region. The aim of the framework is to increase the resilience by identifying potential risk scenarios, develop contingency plans for the relevant scenarios and a general approach to crisis management “if everything else fails”.
- 1.2.3 The actual procedures (including emergency response procedures) **are not** within the scope of this document.

1.3 DOCUMENT MAINTENANCE

- 1.3.1 This document has been adopted by the European Aviation System Planning Group (EASPG) at its fifth meeting in November 2023. The document is published as an ICAO EUR Document on the ICAO EUR/NAT Office website.
-

CHAPTER 2. DEFINITIONS & ACRONYMS

Table 1: Definitions

Disruption	An event or condition that has a significant negative impact on operations
Contingency	A (prolonged) state of non-nominal operations
Crisis	A state where nominal and contingency procedures and resources are no longer adequate
Resilience	A set of properties that: <ul style="list-style-type: none"> • Protects against disruption • Support a quick recovery after a disruption
Air Transportation System	The complete set of elements that are necessary for the execution of air transport as defined in the Chicago convention, e.g.: Aerodromes, Air Traffic Services, Airspace Users
RACI tables	Responsible, Accountable, Consulted, and Informed (RACI) tables
EUR Region	ICAO European Region
NAT Region	ICAO North Atlantic Region

Table 2: Acronyms

ACI	Airport Council International
ADS-B	Automatic Dependent Surveillance - Broadcast
ADS-C	Automatic Dependent Surveillance - Contract
ANS	Air Navigation Services
ANSP	Air Navigation Service Provider
AOC	Aircraft Operator Certificate
ATCO	Air Traffic Controller
ATFM	Air Traffic Flow Management
ATM	Air Traffic Management
CANSO	Civil Air Navigation Services Organisation
CAPSCA	Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation
CCT	Crisis Coordination Team
CCTV	Closed Circuit Television
CNS	Communication Navigation Surveillance
DGCA	Directors General of Civil Aviation
EACCC	European Aviation Crisis Coordination Cell
EASA	European Union Aviation Safety Agency
EASPG	European Aviation System Planning Group
ECDC	European Centre for Disease Prevention and Control
ERP	Emergency Response Plan

ESA	European Space Agency
EU	European Union
EUROCONTROL	European Organisation for the Safety of Air Navigation
FIR	Flight Information Region
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
IAEA	International Atomic Energy Agency
IATA	International Air Transport Association
ICAO	International Civil Aviation Organization
NASA	National Aeronautics and Space Administration
NM	Network Manager
PANS	Procedures for Air Navigation Services
RCS	Risk Classification Scheme
SARPS	Standards and Recommended Practices
SLA	Service Level Agreement
SRA	Safety Risk Assessment
SWXC	Space Weather Centre
UN	United Nations
VAAC	Volcanic Ash Advisory Centres
VOLCEX	Volcanic Ash Exercise
WHO	World Health Organisation
WMO	World Meteorological Organisation

CHAPTER 3. RISK MANAGEMENT

3.1 RISK REGISTER

- 3.1.1 It is highly recommended to create and maintain a Risk Register, containing the relevant risk information for each of the identified scenarios. This risk register should be reviewed regularly as part of the business continuity process.

3.2 RISK ASSESSMENT

- 3.2.1 Risk is commonly defined as a combination (product) of likelihood and impact of an event. This is also the case in a contingency context. In contrast to common (economic) risk assessments, where likelihood and impact are equally weighted, contingency situations have some particularities.
- 3.2.2 Contingency situations, fortunately, have a low occurrence likelihood. Humans are known to have problems dealing probabilistic events, especially with low likelihood events. In addition to these low base rates, the impact variation can be very high, and the impact mechanisms are often not very well understood. For this last group of scenarios, further research is necessary to enable better risk contingency risk assessments.
- 3.2.3 The shortcomings above lead to the application of incorrect probability distributions with subsequent underestimations (Black Swan effect). This is one of the reasons that contingency situations escalate into a crisis.
- 3.2.4 To complicate things further, the (political and public) response to disruptive events is non-linear and depends highly on the visibility of the event.
- 3.2.5 Another difference between common risk assessment and crisis risk assessment is that in the first case the risk is determined to mitigate it. Crisis situations often emerge because the disruptive events were not sufficiently mitigated. This means that for crisis situations, the impact is far more important than the likelihood, because the risk has already materialised.
- 3.2.6 It is important to understand that there is a difference between contingency and crisis risk. The contingency risk is defined by the impact of a given scenario and the occurrence probability of this scenario. The crisis risk is determined by the contingency risk and the risk that the contingency measures are not sufficient.

3.3 RISK MITIGATION

- 3.3.1 **Figure 1** summarizes the essential risk management elements. The risk assessment is described in section 3.1.
- 3.3.2 The mitigation steps that need to be taken depends on the acceptability of the risk. Therefore, criteria need to be defined.
- 3.3.3 It should also be understood that any action taken comes with consequences. The effective and efficient mitigation of a contingency or crisis situation requires a full evaluation of the consequences of an intended action. An example is balancing safety and economic consequences of an action.
- 3.3.4 An alternative approach to the “classical” risk mitigation by direct intervention of the competent authority is through the application of the Safety Risk Assessment (SRA) approach that is currently used in the EUROCONTROL Member States for volcanic ash situations. It leaves the decision whether to fly under volcanic ash conditions to the airspace user, based on an SRA performed by the airspace

user and approved by the competent authority. This way the authorization remains with the State and the operational decisions are taken by the airspace user.

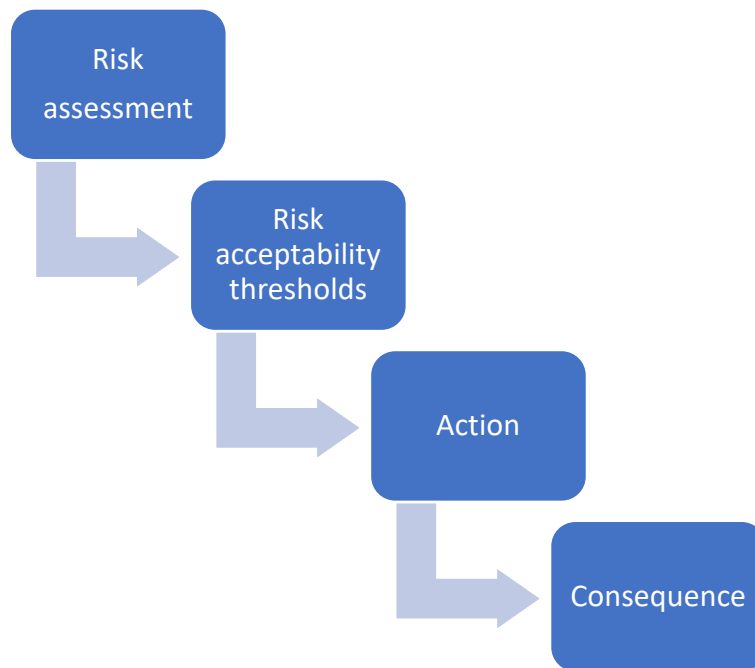


Figure 1: Risk management elements

3.4 RISK ACCEPTANCE CRITERIA

3.4.1 The starting point of risk mitigation is the definition of risk acceptance levels. This can be a complicated task. This complexity often leads to criteria like *ALARP* (As Low As Reasonably Practicable). Such criteria have major flaws such as:

- What is reasonable?
- What is practicable?

3.4.2 In fact, such criteria are procrastinating the decision-making process to the crisis situation. Exactly where you don't want this to be. A contingency situation or crisis can be handled much more effective and efficient with clear decision criteria.

3.4.3 This is also the case for the risk classification scheme (RCS) as shown in . Risk classification schemes are useful for illustrative purposes, but not for decision support. Their linear structure does not match the reality very well. Is a (5,5) risk twice as large as a (3,4) risk? Further, it is not guaranteed that (3,4) risk is the same as a (4,3) risk. This means that the risk classification scheme may be non-monotonous.

3.4.4 To be useful the risk acceptance criteria should have two properties:

- a) They must be unambiguous. When different persons are looking at the criteria, they must have the same interpretation and understanding.
- b) They must be measurable in some form. It must always be clear whether the criterion is met or violated.

3.4.5 Ideally, the risk should be quantified, and in some scenarios this is possible. This is the case in scenarios that are mainly driven by laws of nature. Examples are space debris space weather, volcanic

ash, and nuclear incident scenarios. In these cases, the hazards can be clearly defined, and the understanding of these hazards depend on the amount of effort spent on analysing them.

- 3.4.6 Unfortunately, other scenarios are depending on so many—often unknown—factors that an analysis in closed form is hardly possible. But even in the majority of these cases, estimators of arbitrary precision can be developed. These estimators can be based on statistical data (own or external), form analogy, or resulting from causal analysis.

3.5 MITIGATION STRATEGIES

- 3.5.1 Since the risk is composed of an impact and a likelihood, it can be mitigated by reducing either:

- a) Likelihood, or
- b) Impact, or
- c) Both

		Impact				
		1	2	3	4	5
Likelihood	5	Low	High	Risk	High	High
	4	Low	Medium	High	High	High
	3	Low	Low	Medium	High	High
	2	Low	Low	Low	Medium	High
	1	Low	Low	Low	Medium	Medium

Figure 2: Risk mitigation strategies

- 3.5.2 The most suitable strategy depends on the type of scenario. Most large-scale scenarios have their origin outside the influence range of an organisation (e.g., natural events). In that case reducing likelihood will not be an option. The only way to reduce the risk will be by reducing the impact.
- 3.5.3 For internal risk factors (e.g., fire), the reduction of likelihood may be feasible by taken adequate mitigation measures.

3.6 MITIGATION CONTROLS

- 3.6.1 Once a risk is identified and assessed, it can be compared to the acceptability value and appropriate actions can be taken. These actions can have a preparatory nature like the creation of contingency facilities and procedures or specific responses in case of an unprepared (crisis) situation.
- 3.6.2 A common framework used for risk control is called 4T:
1. Terminate
 2. Treat
 3. Transfer
 4. Tolerate
- 3.6.3 The optimal solution would be to terminate the risk. This can only be done by fully eliminating the cause or the subject of the risk. Although this would be the best option it is often not feasible.

- 3.6.4 The next best option would be treating the risk, for instance by modifying systems or procedures. This treatment can be using all three risk mitigation strategies described in section 3.5 above.
 - 3.6.5 The third option is to transfer the risk. In this case the risk itself does not change, therefore this option has a limited effectivity. A usual way of risk transfer is insurance. This reduces only certain aspects of a contingency or crisis situation (i.e., the financial impact).
 - 3.6.6 The last option isn't often a real one. In some cases, there is no way to reduce the likelihood or impact or only at a prohibitively high cost. In those cases, the only option is to tolerate the risk.
 - 3.6.7 Whatever option is chosen (especially when tolerating the risk), it is always important to document the rationale behind the choice.
-

CHAPTER 4. RESILIENCE, CONTINGENCY, AND CRISIS

4.1 OBJECTIVE

- 4.1.1 The objective of this document is to support the resilience of the air transportation network or in other words reduce the impact of disruptive events on air transport operations through guidance material.
- 4.1.2 One of the most crucial elements in achieving this is to avoid entering a “crisis” mode. As per definition a crisis is a state where the available procedures are no longer adequate to handle the situation.
- 4.1.3 The best way to avoid crisis situations is to prepare for the relevant disruptive events (scenarios). This preparation should be aimed establishing a plan for responses within a harmonised regional framework.
- 4.1.4 The crisis potential of a scenario depends mainly on the direct or indirect impact on aviation. This impact depends on factors like the geographical area, duration, and predictability. Further factors that may contribute to a crisis are public perception, media attention, and politically motivated decisions.
- 4.1.5 A crisis can be triggered by an event that directly affects aviation (e.g., volcanic eruption) or by the response to an event that does not directly affect flight operations (e.g., pandemic).
- 4.1.6 Adequate preparation will not prevent disruptive events from occurring, and these events may and most probably will have an impact on aviation. The difference is that a prepared organisation will transition into a controlled contingency mode instead of entering a crisis.

4.2 EVENT LIFE CYCLE

- 4.2.1 Disruptive events usually have similar life cycles, regardless of the type of event. The main difference between the life cycles is whether there is a warning period. The presence (or absence) of a warning period determines the safety impact and the gracefulness of the transition to the contingency phase.
- 4.2.2 A severe disruption occurs without warning may lead to a “safety” phase. This, usually short, phase requires immediate action that is described in the Emergency Response Plan (ERP). This ERP is out of scope of this document.
- 4.2.3 After the safety is ensured, the contingency procedures should be activated.

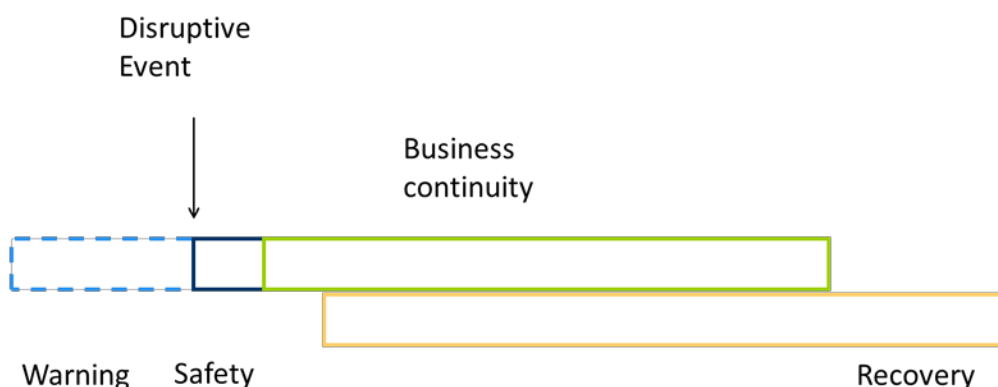


Figure 3: Contingency phases

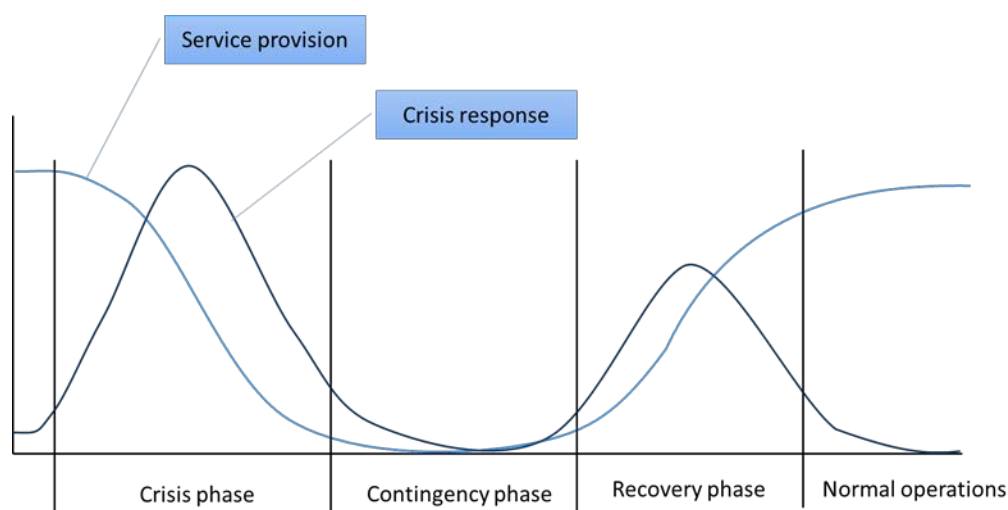


Figure 4: Service provision and crisis response

4.2.4 Figure 4 shows the typical relationship between the level of service provision and the crisis response effort. Crisis response is most intense in situations where the service provision levels change. The COVID-19 crisis showed that even in case of persisting low levels of traffic, the crisis response and corresponding support needs quickly declined after the stabilization of the traffic levels. It is, therefore, recommended that the crisis teams are de-activated as soon as the situation becomes stable (i.e., no big changes). De-activation means that they are taken out of the decision chains.

4.2.5 It is also important to understand that the changes in a positive direction will also often require support from the crisis team. Therefore, it is recommended that the de-activated crisis team remain available until the situation is restored to a sufficient level to be picked up by the regular organisation.

4.3 CRISIS MANAGEMENT PLAN

4.3.1 As per definition, a crisis is a state where the normal and contingency procedures are no longer adequate. It, therefore, does not make sense to try and define yet another set of scenario related procedures.

4.3.2 The crisis management plan only should contain a set of high-level procedures that clarify roles and responsibilities and communication channels during a crisis situation¹.

4.4 CONTINGENCY PLAN

4.4.1 ICAO Annex 11 — Air Traffic Services, states (in section 2.32 - Contingency arrangements) that air traffic services authorities shall develop and promulgate contingency plans for implementation in the event of disruption, or potential disruption, of air traffic services and related supporting services in the airspace for which they are responsible for the provision of such services. Such contingency plans shall be developed (with the assistance of ICAO as necessary) in close coordination with the air traffic services authorities responsible for the provision of services in adjacent portions of airspace and with all airspace users concerned. Annex 11 Attachment C provides further guidance material relating to the State's responsibilities, status, development, promulgation, coordination, implementation and application of contingency plans.

¹ If the contingency procedures are adequate, a crisis should be an extremely rare event.

- 4.4.2 Furthermore, the Commission Implementing Regulation (EU) No 2017/373 specifies in part ATM/ANS.OR.A.070 (Contingency plans) that a service provider shall have in place contingency plans for all the services it provides in the case of events which result in significant degradation or interruption of its operations. As part of the EASA Basic Regulation (EU) 2018/1139, article 43a, and Annex VIII specify that a service provider shall establish and implement a contingency plan covering emergency and abnormal situations that may occur in relation to its services, including in the case of events which result in significant degradation or interruption of its operations. (see more details in EASA ATM/ANS OR. A.070 and EASA ATS OR.135)
- 4.4.3 The contingency plan should normally consist of two major elements, a contingency preparation plan and a contingency execution plan.
- 4.4.4 Contingency preparation plan
- 4.4.4.1. The contingency preparation plan contains the following :
- Requirements both from regulatory bodies and stakeholders. These requirements are the starting point for the determination of scenarios and mitigation means.
 - Required resources based on the identified scenarios and required mitigations
 - All relevant scenarios. In principle at least all scenarios in ICAO EUR Doc 031 should be taken into consideration². If particular scenarios should not be applicable this should be explicitly justified.
 - Training plan containing the training requirements for all potentially involved staff (not only the crisis or contingency management team)
 - Regular exercises for all applicable scenarios.
- 4.4.5 Contingency execution plan
- 4.4.5.1. The contingency execution plan contains all relevant scenarios and the procedures that have to be applied to handle each scenario.
- 4.4.5.2. These procedures should include, but are not limited to:
- Operational procedures
 - Technical procedures
 - Organisational procedures
 - Communication procedures
- 4.4.6 These procedures should be trained and exercised regularly.

4.5 EVALUATION AND “LESSONS LEARNT”

- 4.5.1 One of the most important, yet commonly underestimated, aspects of crisis management is a thorough evaluation of a contingency or crisis.
- 4.5.2 This evaluation is always important, regardless of the crisis or contingency response going well or less so. The lessons learnt from the evaluation are more effective than anything that can be taught from theory.
- 4.5.3 Therefore, the contingency and crisis management plans should explicitly address the post event analysis. The following should be included in the plan:

² The scenarios in this document comprise a “minimum set” and do not claim to be complete.

Clear instructions for collecting information and communications during the event.

- What happened?
- Event timeline
- Actions taken
- Communications

4.5.4 The evaluation should be done as quickly as possible after the event and should be executed in a “no blame” culture.

4.5.5 The plan should also address the feedback from the evaluation to the crisis management and regular organisation.

4.5.6 Typically, this would result in updates of:

- Processes
- Documentation
- Training
- Exercises

4.6 NON-EVENT RELATED ACTIVITIES

4.6.1 The success of contingency and crisis management activities depend mainly on the level of preparedness. Preparedness consists of two elements:

- a) Awareness of the situation
- b) Understanding of the impact of specific scenarios

4.6.2 The situational awareness requires a continuous evaluation of the developments in the environment of the organisation. This can be environmental developments (e.g., solar cycles, weather/climate, wildfires etc.), criminal developments (e.g. cybercrime) or political developments (e.g. escalation of international tensions). In fact, all factors that can contribute to the escalation of a specific scenario should be monitored.

4.6.3 The monitoring and evaluation of scenarios requires a good understanding of the factors contributing to each scenario and the mechanisms behind them. In many cases this requires a certain degree of research and training, which should take place regularly.

CHAPTER 5. IMPLEMENTATION ASPECTS

5.1 INTRODUCTION

- 5.1.1 The ability to respond adequately to a disruption depends to a large extent on the maturity and preparedness of an organisation. Adequate procedures that are trained and exercised are essential for an affective contingency response. If the situation escalates beyond a contingency situation, procedures will—except for a few basic rules—not be effective. In this situation a clear definition of the roles and responsibilities of all involved stakeholders is the most important piece of information. During a disruptive event and especially during a crisis good communication is essential and should be addressed in a dedicated communication plan.

5.2 TRAINING

- 5.2.1 Contingency and crisis situations are, by definition, anomalies. This means that persons involved in such situations do not have a natural proficiency. On the other hand, these situations often require a quick response to limit the damage.
- 5.2.2 The proficiency needs to be ensured through training and exercises. The training should not only involve the crisis management staff, but also the regular staff. At least to the extent that the interface between crisis and regular organisation is well understood by all persons involved.
- 5.2.3 The training should follow the structures in the contingency and crisis management plans. A generic course without a clear link to these plans is not very effective³.
- 5.2.4 Training objectives should be:
- Staff proficiency on contingency and crisis procedures
 - Cooperation with (inter)national crisis structures
 - Cooperation with (inter)national expert organisations
 - Communication during contingency and crisis organisations
- 5.2.5 The training plan should contain the definition of training requirements based on the objectives above, refresher intervals, training methods. The training intervals should not be too large and new staff should receive the training as part of the induction process.
- 5.2.6 Training methods can be chosen as appropriate:
- Classroom training
 - On-the-job training
 - Computer based (online) training

5.3 EXERCISES

- 5.3.1 The exercises are an extension of the training and should follow the contingency and crisis management procedures. The purpose of the exercises is:
- Validating the contingency and crisis management procedures
 - Checking preparedness of the organization
 - Testing the cooperation with external stakeholders
- 5.3.2 The format of the exercises can vary depending on the objective and capabilities of the organization.

³ This is important when considering a training from an external provider.

5.3.3 Common examples are:

- Desktop exercises
 - Static (scripted without injects)
 - Dynamic (scripted with injects)
- Live exercises
 - Computer simulations
 - Simulated physical situations

5.3.4 All these exercises have their particular focus. More important than the format is the quality and regularity of the exercises.

5.3.5 Participation of all relevant stakeholders should be ensured. Simulating stakeholders creates the risk of surprises during a real event because the assumptions about a reaction during the exercise may not have been correct.

5.3.6 Since the preparation of an exercise is time and effort consuming, it is recommended to cooperate closely with other stakeholders (adjacent centres, airports, airlines) and rotate the “organizer” role. This does not only reduce the effort, but also introduces different perspectives.

5.4 ROLES & RESPONSIBILITIES

5.4.1 Separate "Responsible, Accountable, Consulted, and Informed (RACI)" tables for contingency and crisis situations. Especially the tables for contingency procedures may depend on the scenario. It is important to consider external roles as well in the RACI. In that case clear interfaces need to be established and agreed with the external entities.

		CEO	COO	CTO	Operations manager	Engineering manager	Operations supervisor	Technical supervisor	Communications	Operational teams	Technical teams
	Contingency plan										
1.1	Analyse all available information related to potential contingency scenarios (Operational)		A		R	I	C			R	
1.2	Analyse all available information related to potential contingency scenarios (Technical)			A	I	R		C			R
1.3	Classify the potential crisis scenarios	A	R	R	C	C	C	C			
1.4	Develop operational contingency procedures			A	A	I	C			R	
1.5	Develop technical contingency procedures				I	A		C			R
1.6	Identify necessary contingency facilities		A		R		C				
1.7	Develop contingency facilities			A		R					
1.8	Establish emergency response teams										
1.9	Create communication plan	A							R		
	Event response										
2.1	Collect information associated with the contingency										
2.2	Assess the situation										
2.3	Initiate emergency response (if necessary)										
2.4	Inform internal and external stakeholders										
2.5	Initiate contingency measures										
2.6	Ensure contingency operations										
	Recovery										
3.1	Initiate the recovery process										
3.2	Determine the recovery options										
3.3	Ensure the availability of recovery resources										

Figure 5: Example of RACI table

5.5 COMMUNICATION

5.5.1 Communication is the most important factor in handling crisis situations. Therefore, the contingency and crisis management plans should have dedicated sections defining the communication during a crisis. A separate communication plan is also an option if it is ensured that this plan is in line with the contingency and crisis management plans. The communication plan should distinguish between:

- Internal communication
- External communication
 - Stakeholders
 - Media
 - General public

5.5.2 Regardless of the target audience the communication should always stick to the facts and use clear language.

5.5.3 Internal

5.5.3.1. Contingency and crisis situations are accompanied by a lot of uncertainty. It is, therefore, essential to keep the staff informed at all times in order to avoid uncoordinated actions and rumours.

5.5.3.2. Communication should be factual and limited to the extent necessary for handling the contingency/crisis. Information overload may reduce the efficiency of staff.

5.5.3.3. It should always be clear for the staff who is authorized to communicate. This should be aligned with the RACI table (see Figure 5). Only communication channels that people are familiar with should be used⁴. It should be ensured that the communication channels that are used have sufficient capacity to handle the increased communication load⁵.

5.5.3.4. It is important that the contingency/crisis communication is ensured for all potential scenarios. This means that the communication channels must be either independent of any external provider or be backed up by a truly independent channel with the same capacity.

5.5.4 External

The external communication should be split into the stakeholder communication and information for the "general public".

5.5.4.1. Stakeholders

- a) The communication with stakeholders is quite similar to the internal communication. It should focus on handling and resolving the situation and should also use familiar communication channels.
- b) The channel capacity is more critical than in case of internal communication since it depends on external providers.

5.5.4.2. Media

- a) The communication with the "traditional" media is normally handled by the corporate communications department. It is, therefore, essential that the staff in this department is fully integrated in the contingency/crisis training and exercises. During a contingency/crisis there is no time to explain the situation at length.
- b) It is recommended to prepare a "press kit" for each identified scenario that includes the background information, so that only the event specific information has to be included.

⁴ Creating a dedicated crisis communication system is not recommended.

⁵ Public communication systems like mobile phone systems may be overloaded during a large crisis.

5.5.4.3. General public

- a) With the introduction of the Internet in general and social media in particular, direct communication channels to the “general public” have become available for all organizations.
 - b) The communication through social media is usually handled by the corporate communication departments and should be kept in line with the communication with the “traditional” media. When using social media, care should be taken in the choice of the platform.
 - c) During a crisis the public attention will increase as will speculation and rumours. It is, therefore, highly recommended to choose an open, factual, and unambiguous communication style to avoid the spread of misinformation.
 - d) The message can be reassuring but should always be honest.
 - e) A sometimes-overlooked communication channel I times of crisis is the “normal” Internet presence (corporate website). When this channel is used to provide information about the contingency/crisis to the general public, it should be ensured that the site can handle the increased traffic.
 - f) If the site provides real-time information from automated systems, it should be checked if this information is not compromised as result of the contingency/crisis.
-

CHAPTER 6. NATIONAL CRISIS MANAGEMENT STRUCTURES

6.1 GENERAL

- 6.1.1 The management of any aviation crisis is a national responsibility and shall be executed by the appropriate national crisis management structure. Depending on the nature of the crisis, the coordination/cooperation between civil and military stakeholders might be a crucial element in the management of a crisis, emergency or disaster.

6.2 NATIONAL STRUCTURES

- 6.2.1 These national structures are diverse across states and are largely determined by the size of the country, the state organisation (e.g., central versus federal), and the political structure in the state.
- 6.2.2 Since aviation related crises very often are transnational, a national aviation crisis management organisation should be organised in a way that supports international cooperation.
- 6.2.3 In practice, this means that information about the national crisis management structures should be regularly exchanged between neighbouring countries and with regional and international crisis coordination structures. In particular the contact details of persons involved in national crisis management.
- 6.2.4 Within each state, the aviation crisis management structure should be embedded in the national crisis management structure. The aviation crisis structure should have immediate access to structures that are responsible for area that are relevant for aviation such as public health, energy supply, national security, alternative means of transport, cyber experts etc.
- 6.2.5 Joint exercises with the different national crisis management structures should be held regularly.
-

CHAPTER 7. REGIONAL COORDINATION

7.1 REGIONAL STRUCTURES

- 7.1.1 As aviation is an international industry, crisis situations will rarely be limited to a single state. This means that for an effective and efficient handling of a crisis, international coordination will be necessary.
 - 7.1.2 The scale of the coordination depends on the scale of the crisis. During the COVID-19 crisis, coordination on a global scale was necessary. Often the crisis situations are regionally constrained.
 - 7.1.3 A good example was the eruption of the Eyjafjallajökull volcano in 2010. As direct result of the crisis following the eruption, a regional crisis coordination structure, the European Aviation Crisis Coordination Cell (EACCC), has been established.
 - 7.1.4 During several large disruptions and crisis situation after its establishment by providing an enhanced level of regional awareness to the states and coordinate in cases where national coordination was not efficient.
 - 7.1.5 An important activity of the EACCC is the organisation of annual crisis management exercises and the support of the ICAO VOLCEX exercises.
-

CHAPTER 8. INTERNATIONAL COOPERATION

8.1 STRUCTURES

- 8.1.1 A key to success in the effective and efficient handling of crisis situations is international cooperation. Although the responsibility of crisis management is a national issue, cooperation has many benefits. Most states, especially in the same region, will often face the same or at least similar challenges. Instead of trying to solve them in isolation, it would be more efficient to look jointly for solutions. Apart from the increase in efficiency, this would also lead to harmonised approaches that have been proven to be more effective than isolated actions.
- 8.1.2 The activation of a tactical Crisis Coordination Teams (CCT) should typically enable the identification of the operational challenges resulting from a crisis and engaging with the relevant local and especially regional stakeholders to ensure safe operations. CCTs are an effective mechanism when the effects of the crisis also impacts States in neighbouring ICAO Regions.
- 8.1.3 There are many international expert organisations that can support the aviation sector in case of disruption and crisis.

8.2 ORGANISATIONS

- 8.2.1 Some examples are UN organisations like:
- World Health Organization
 - World Meteorological Organization
 - International Atomic Energy Agency
- 8.2.2 In addition to these global organisations, regional expert organisations should be used to provide support in case of disruption or crisis situations.
- 8.2.3 Here we also should indicate that contingency management should be done in close cooperation. Since states are mainly facing similar problems, it is easy to achieve significant synergies by cooperating
-

CHAPTER 9. SCENARIO CATEGORIES

The aim of categorising the response is to facilitate the response. Since there are multiple ways of categorising, this should only be seen as a possible example. Other classification schemes can be considered as well.

9.1 INTERNAL

9.1.1 In this category, the event is internal. Normally the scope of such an event will be local or national. In contrast to the external events, the affected organisation has a larger influence on the event.

9.2 EXTERNAL

The majority of events that have contingency or crisis potential will be external.

9.2.1 Natural

9.2.1.1. In case of natural events, there is hardly anything that can be done to reduce the likelihood of the event. The only option is to be prepared for these types of events.

Disruptive event	Crisis potential
Fire	Fire is, in general, a local phenomenon with limited crisis potential. An exception could be the simultaneous outbreak of wildfires affecting essential services or critical infrastructures.
Flood	Floods are, usually, local phenomena and therefore only have limited crisis potential.
Earthquake	Earthquakes are also local phenomena. Their crisis potential results from the massive damage that can result from an earthquake. Depending on the location, this could mean that essential services or critical infrastructures can be unavailable for extended periods of time.
Severe weather	Severe weather can affect relatively large geographical areas. The good understanding of weather phenomena and experience with responses limit the crisis potential. Climate change, however, may lead to regionally uncommon weather phenomena.
Space weather	The potentially large geographical areas and the limited understanding of severe space weather event impact on aviation, increases the crisis potential.
Space debris	The understanding of space debris on aviation is still limited, but studies indicate that the risk is generally low. Depending on the trajectory and size of the re-entry object, a case specific risk assessment has to be performed. The main problems are the uncertainty in forecast and over-reaction in the response. Overall, the crisis potential is low.
Volcanic ash	Experience has shown that volcanic ash events had a significant crisis potential in the past. The common acceptance of the SRA has reduced the crisis potential, but the disruptions can be very significant.

9.2.2 Infrastructure

9.2.2.1. The situation in case of infrastructure outage is a bit different. In general, organisations have a certain level of influence in setting up their infrastructure or at least reducing the dependency and increasing redundancy.

Disruptive event	Crisis potential
Electrical power unavailability	Local power supply issues will not create a network crisis, but regional or pan-European power outages can have a severe impact, lasting days to potentially weeks. Local Uninterruptible Power Supply (UPS) systems are not able to mitigate large scale power outages.
Fuel supply unavailability	The supply of (jet) fuel depends itself on local factors, like transportations and international factors like fuel production. A disruption of the latter and, to a lesser extent the former, have the potential to create a crisis.
Communication networks unavailability	With increasing connectivity, communication network failures are becoming an increasing risk. Large scale communication failures can like large scale electrical power failures have a societal impact and trigger an aviation network crisis.
GNSS degradation or unavailability	Satellite navigation is becoming a core service used across the transportation domains. Initially it was limited to one provider (GPS). Nowadays, multiple providers are available although not all users are able to use all alternatives. Being a space-based service, GNSS is susceptible to space weather events, which may lead to common mode failures. It should be noted that static terrestrial systems are depending on GNSS for accurate time information.
Air traffic management unavailability	Air traffic services are related to airports and FIRs. An unavailability of an ANSP will normally not be sufficient for triggering a crisis. If multiple ANSPs are not available due to a common underlying cause (e.g. cyberattack), a crisis is possible. An exception to the "local" scope of air traffic management services is the Network Manager. A medium- or long-term outage of NM will lead to severe disruptions, up to a crisis level.
Airline operations services unavailability	Airline operations services are comparable with ANSPs. A single outage may not be sufficient for a crisis, but the loss of multiple Airline Operations Centers may trigger a crisis.
Airport unavailability	Unavailability of a limited number of airports for a short period of time (hours) is not uncommon and not a trigger for a crisis. A longer unavailability of (days) a larger number of airports may create a crisis. This could be caused by a severe weather condition in a large geographical area.
Meteo services unavailability	Meteo services are essential for safe air transport. Outage of multiple meteo service providers may cause serious disruption, but the crisis potential is limited.

9.2.3 Man-made

9.2.3.1. In case of man-made events, it is often not the event itself but the political or societal response that causes the disruption. This means that the responses to such events are also often "non-technical".

Disruptive event	Crisis potential
Pandemic⁶	COVID-19 has shown that a pandemic has a large crisis potential. It should be noted that the crisis is the result of a response to a societal risk.
Terrorist attack	A terrorist attack may directly affect flight operations if targeted on aviation. This will normally not have a network wide impact. Large scale responses however may create a crisis situation.
Armed conflict	An armed conflict may affect a medium sized or large geographical area. Immediate responses to the conflict may trigger a network crisis.
Political tension/conflict	Even without an armed conflict, political tension may lead to responses that can heavily affect air transport, thus triggering a crisis.
Cyber-attack	A cyber-attack can disable important essential services or critical infrastructures. This would directly trigger a crisis.
Nuclear incident	A nuclear incident is a local event, but atmospheric dispersion of radiation can cover significant geographical areas. The main crisis potential comes from the uncertain responses by national authorities. The reaction of the general public (i.e. mass cancellations), may also lead to a crisis.
Chemical incident	Chemical incidents are similar to nuclear incidents. The crisis potential is lower than from a nuclear incident, mainly due to lower media attention. In this case the crisis would be triggered by the response to the incident.
Drone activity	Drone activities near airports can be very disruptive. In case of a coordinated action, this can lead to a crisis situation. Also, the anticipation of a coordinated action can trigger a crisis situation

⁶ Strictly speaking, a pandemic is not a man-made event. The main impact for aviation, however, comes from man-made decisions.

APPENDIX A – SCENARIOS

1. List of identified scenarios with a high-level description of the impact on aviation.
2. This should be seen as examples. It is very difficult to create an exhaustive list. The contingency and crisis management processes should be developed in a way that provides sufficient flexibility to respond to unexpected events.
3. It should be clear that the list provided in this document is only an example. Depending on the national and regional situations other or additional scenarios need to be considered or some of the listed scenarios are less relevant. The scenario list is not static and needs to be reviewed regularly.

~~~~~

## 1 CRI-001 – FLOODS

Floods are usually local events. The impact on aviation is indirect as result of the unavailability of general or aviation infrastructure.

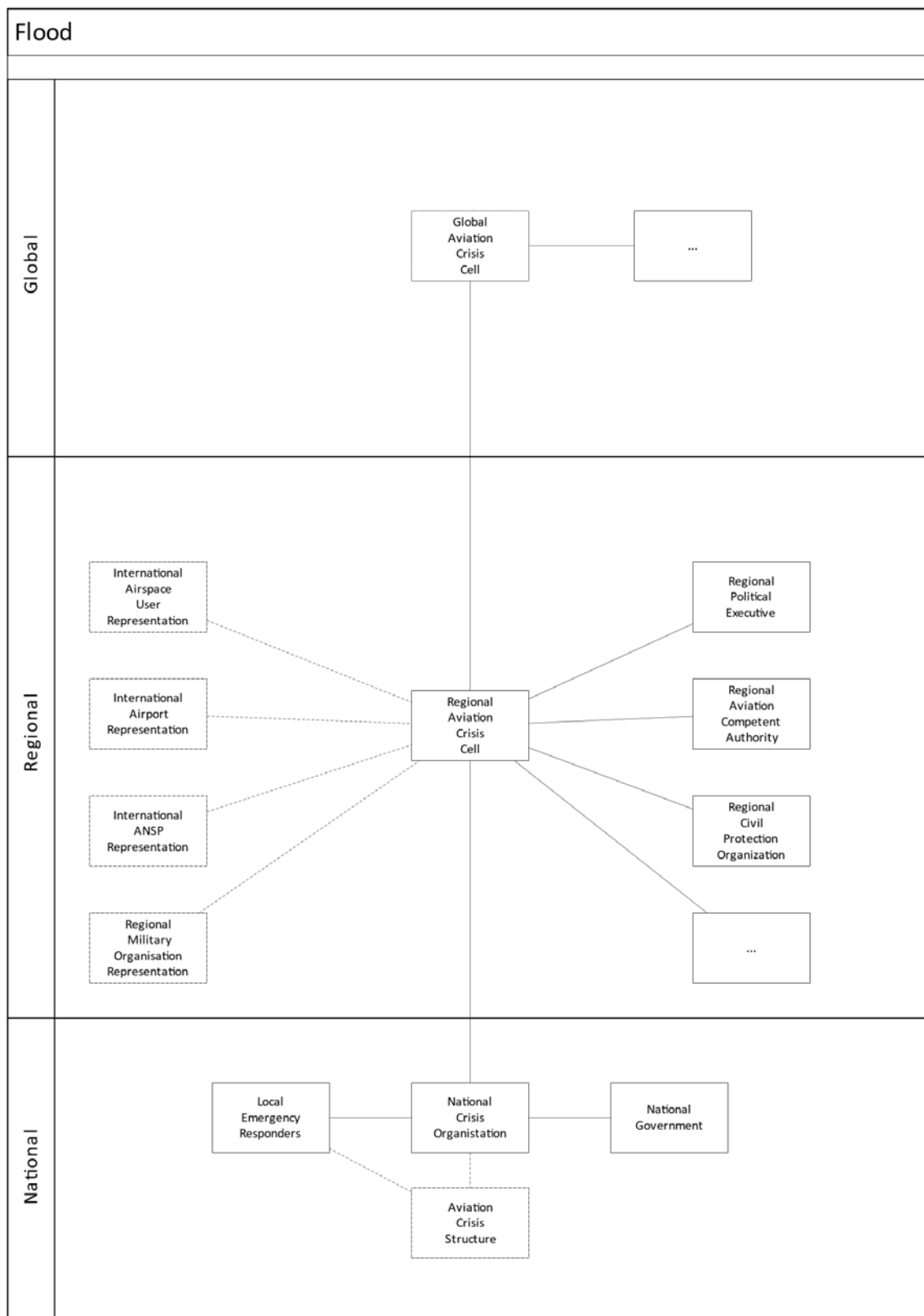
In most of the cases, the aviation impact of a flood can be handled on national level (or in direct coordination with neighbouring states).

How to determine the risk:

- Different types of flood risk:
  - Flash flood after excessive rain
  - Flood risk by large water bodies (rivers, lakes, sea)
- Investigate the likelihood for each of the flood types
- Assess the potential impact for each of these flood types

How to mitigate the risk:

- Define mitigation means for each flood type
  - Flash flood may be mitigated by local contingency measures
  - Flood risk by large water bodies may require external contingency facilities



## 2 CRI-002 – EARTHQUAKE

Earthquakes are usually local events. The impact on aviation is indirect as result of the unavailability of general or aviation infrastructure.

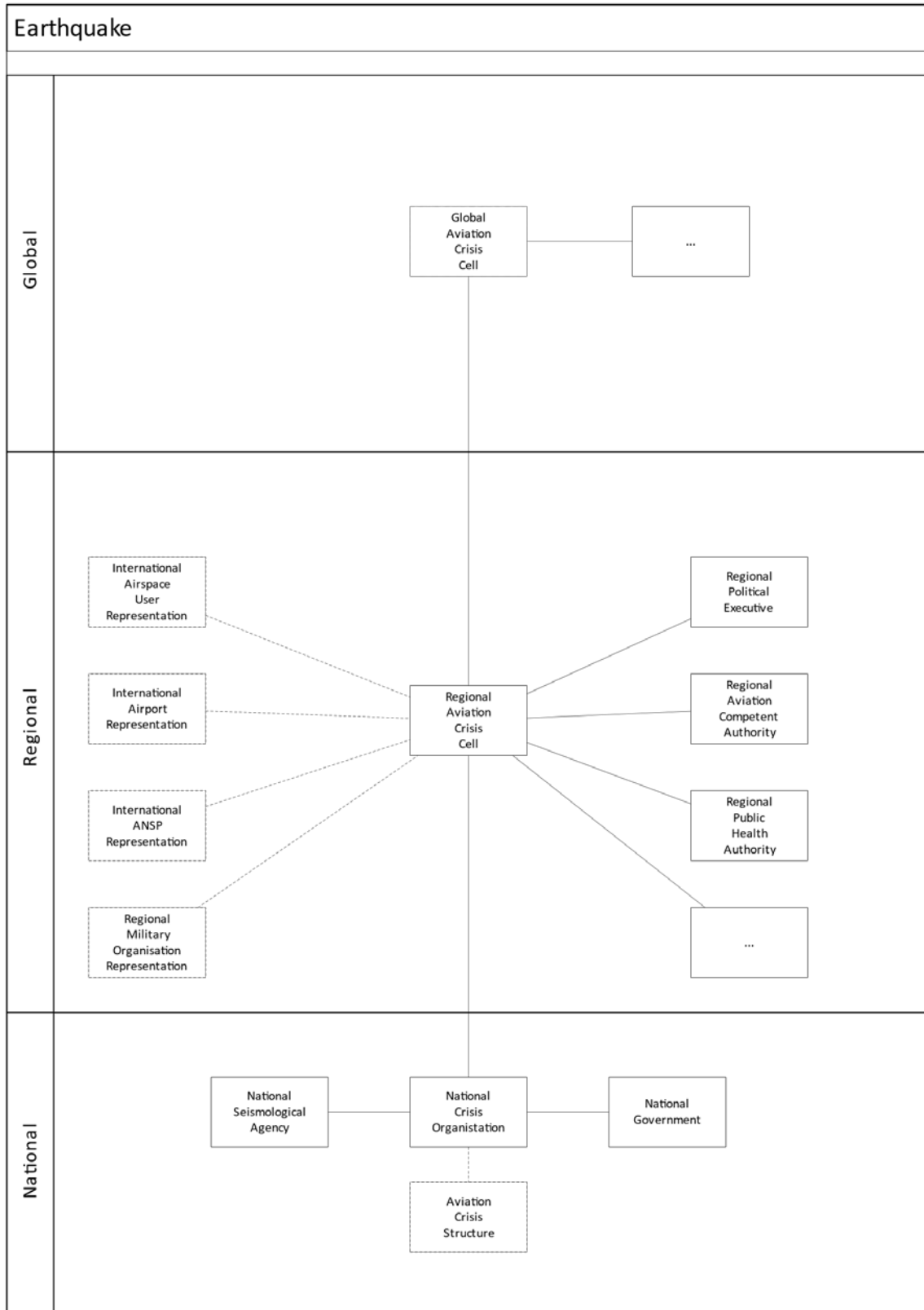
In most of the cases, the aviation impact of an earthquake can be handled on national level (or in direct coordination with neighbouring states).

How to determine the risk:

- Consult the national seismological survey
  - This gives information about the likelihood and severity of the earthquakes
  - Sometimes this is handled by the national meteo institution
- Check the building and infrastructure designs for earthquake resilience
  - This gives information about the impact of a potential earthquake of a given magnitude

How to mitigate the risk:

- Avoid locations that are close to known geological faults
- Ensure that the buildings and other infrastructure elements are designed to sufficient limits
- Ensure that there is sufficient distance between main and contingency facilities





### 3 CRI-003 – VOLCANIC ASH

Volcanic ash is widely recognized as a safety hazard for aviation. High concentration of ash can deteriorate the performance of engines and scratching the cockpit windows. Even low to medium concentrations can cause damage to the engines in case of longer exposure. Therefore, flights into volcanic ash clouds should be avoided.

Guidance for dealing with Volcanic Ash situations can be found in the ICAO Volcanic Ash Contingency Plan (VACP).

In the EUROCONTROL Member States, a Safety Risk Assessment (SRA) approach has been adopted that allows the airline operators to operate in volcanic ash situation within the limits of the SRA approved by the competent authority.

Although the eruption itself is a local event it can have a regional impact on aviation because large airspace may become unavailable due to ash contamination. Therefore, regional coordination may be necessary.

How to determine the risk:

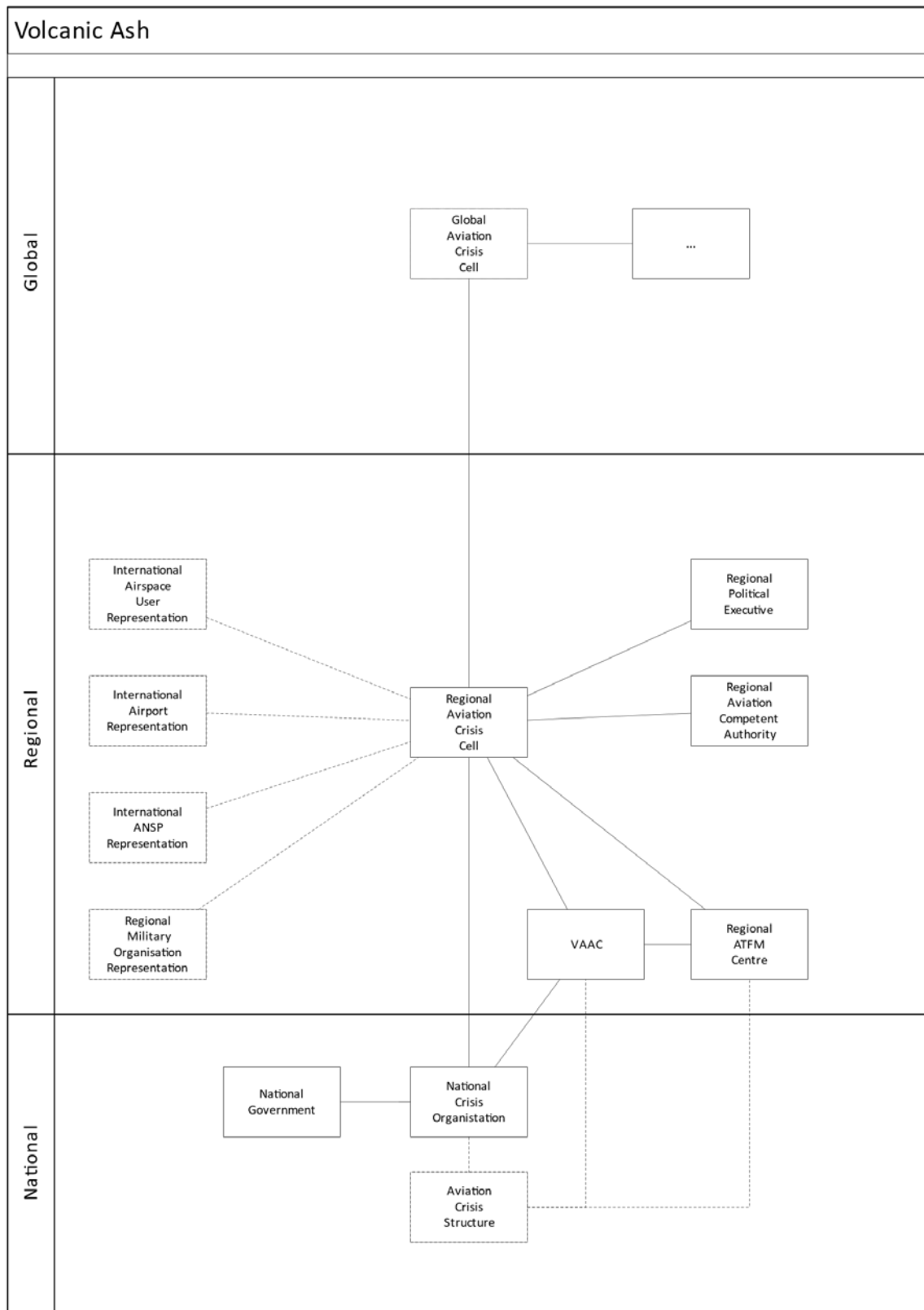
- Check the existence of volcanoes in the area<sup>7</sup>
- In case of eruptions consult the advisories from the Volcanic Ash Advisory Centres (VAAC)

How to mitigate the risk:

- The immediate response to an volcanic eruption is well described in the ICAO VACP
- It is highly recommended to introduce and adhere to an SRA approach

---

<sup>7</sup> Note that the area should be widely interpreted. Volcanic ash can travel several thousand kilometres in damaging concentrations.



#### 4 CRI-004 – NUCLEAR INCIDENT

A nuclear event is normally a local event. Like in case of volcanic ash, aviation can be impacted by the unavailability of airspace due to radio-active contamination. The mechanism of cloud dispersion is similar to volcanic ash, but in general the contaminated airspaces are smaller than in case of a volcanic eruption.

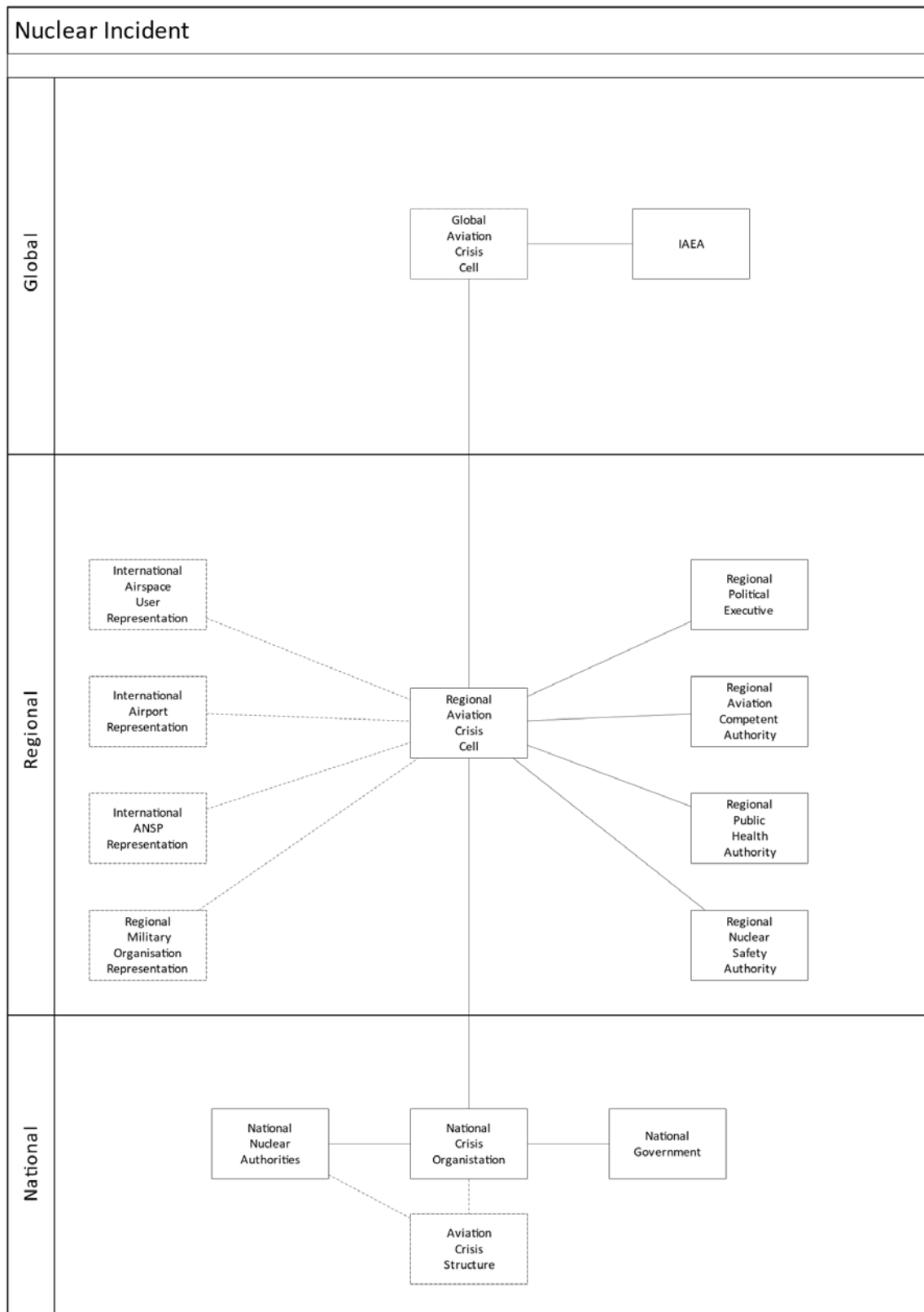
Although the event has a local origin, regional coordination may be necessary.

How to determine the risk:

- Check for nuclear facilities in the vicinity
  - For example, by contacting national nuclear regulatory bodies or IAEA
- Investigate the resilience of site against small or distant nuclear incidents
  - Large and nearby incidents will lead to immediate and long term evacuation

How to mitigate the risk:

- Small or distant incidents
  - Install radio-active particle filters in the air intakes
- Large or nearby incidents
  - Create long term evacuation plans
- The main difference between nuclear and conventional events is that the evacuation duration can be much longer (years), making a return practically impossible.
- This means that for affected centres a contingency facility should be chosen that is certainly outside the danger area.



## 5 CRI-005 – ARMED CONFLICT

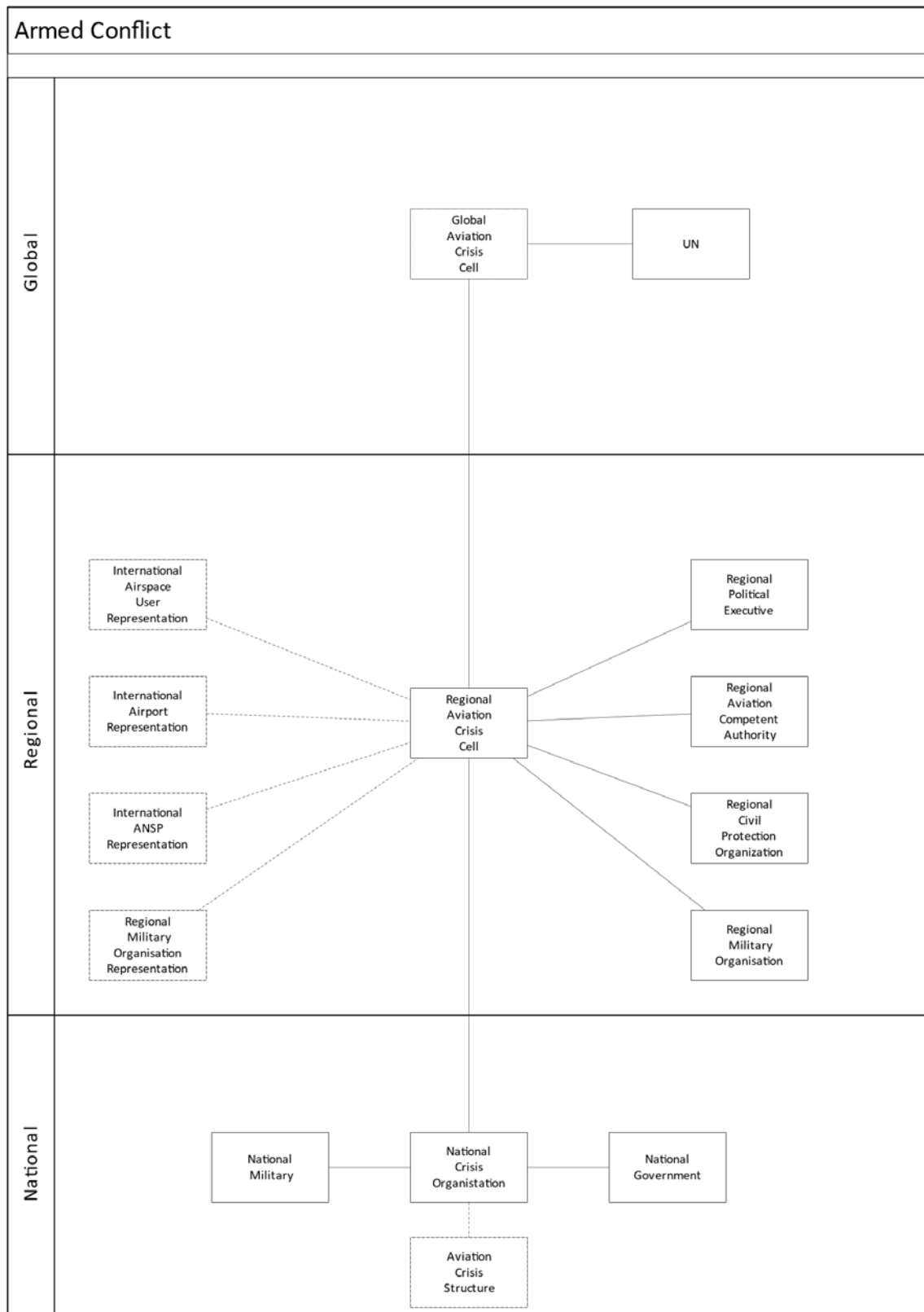
Armed conflicts usually involve multiple states and are, therefore, regional scenarios. Apart from the directly affected states, an armed conflict may have impact on aviation in adjacent states as well. The political tension resulting from a conflict may result in effect even beyond this area.

How to determine the risk:

- Gather intelligence from media and diplomatic channels
- Analyse the impact of likely scenarios on aviation

How to mitigate the risk:

- Prepare responses for the identified scenarios (e.g. alternative routing)
- Make arrangements with adjacent states



## 6 CRI-006 – DANGEROUS CHEMICAL INCIDENT

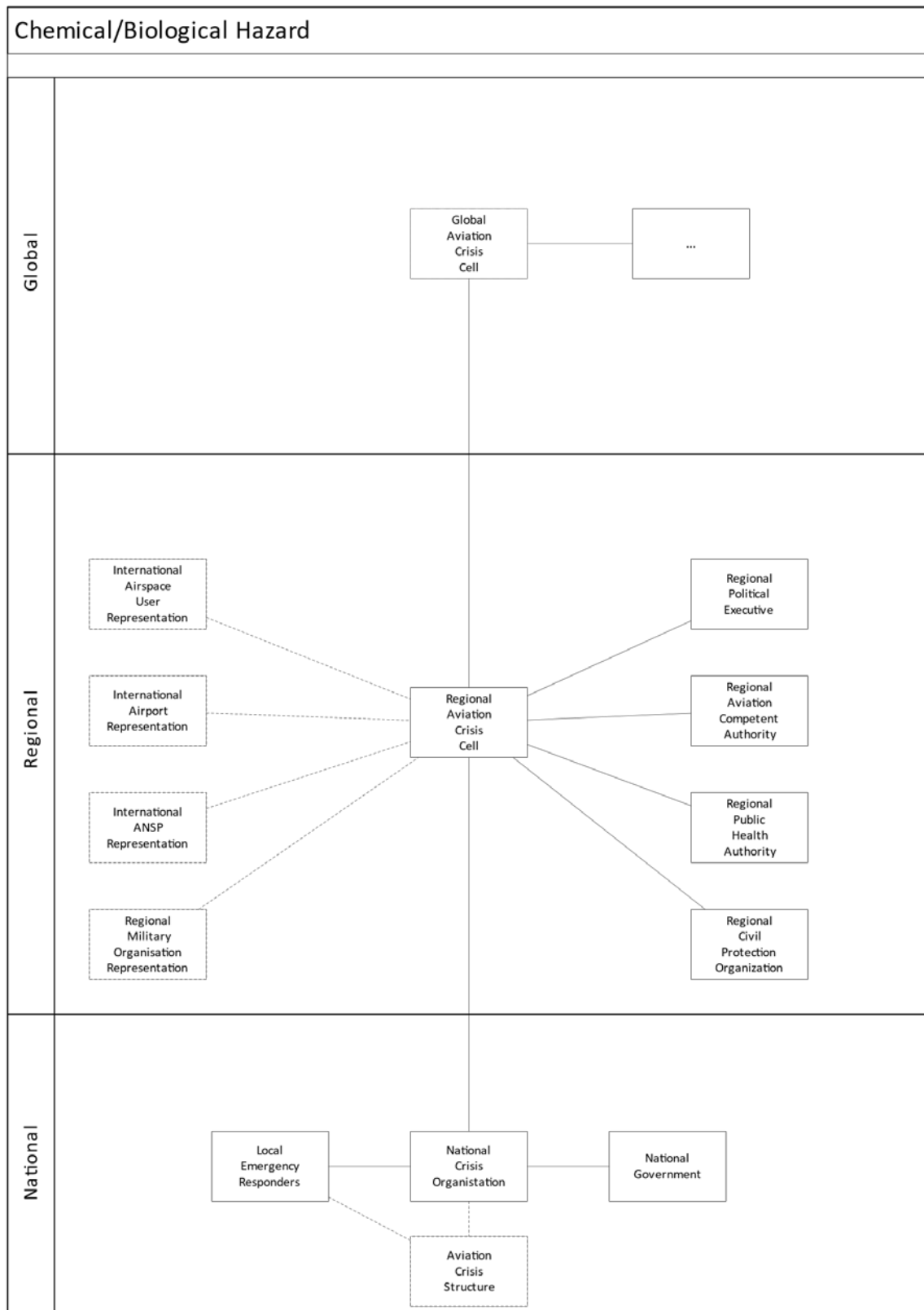
Dangerous chemical incidents are local events with a limited spread. Although the dispersion mechanisms are like those of volcanic ash and nuclear incidents, the likelihood of regional contamination is significantly less. A regional impact could happen if the chemical incident leads to the unavailability of an important part of the regional aviation infrastructure.

How to determine the risk:

- Survey of chemical industry in the environment
- Source can be regional/local authorities
- Unmitigated impact can be derived from distance, types of chemicals
- Likelihood can be determined from the chemical plant's own risk assessment and the prevailing wind directions

How to mitigate the risk:

- Since this threat normally comes from external sources, it is difficult to influence the likelihood, therefore the mitigation should emphasize on reducing the impact.
- Depending on the health risk (e.g. irritation or significant health risk), available time and duration:
  - Evacuation procedures
  - Sealing of the building
  - Active carbon filters





## 7 CRI-007 – FIRE

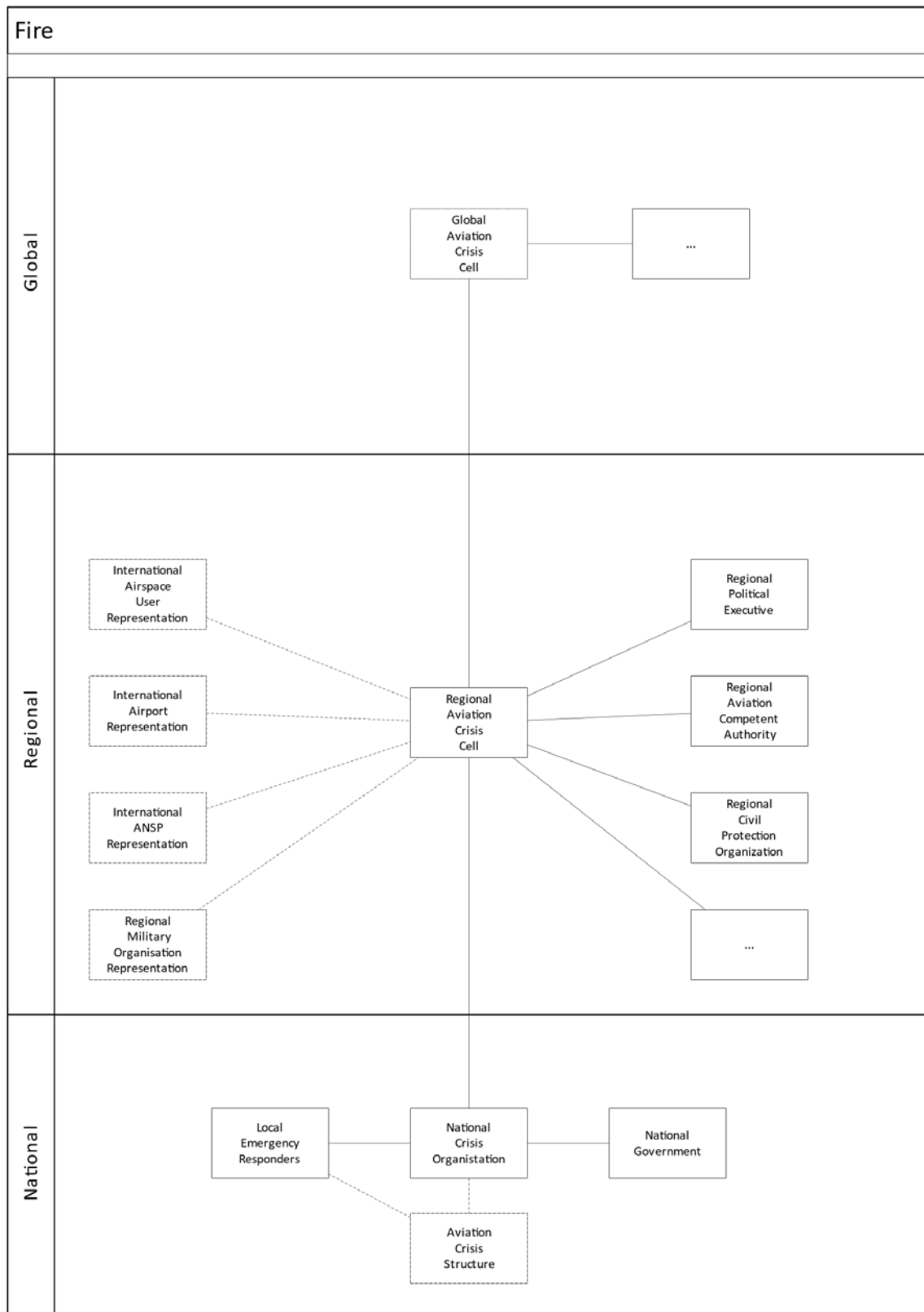
Fires are local events and only have impact on aviation if important parts of the national or regional aviation infrastructure become unavailable.

How to determine the risk:

- Survey of chemical industry in the environment
- Source can be regional/local authorities
- Unmitigated impact can be derived from distance, types of chemicals
- Likelihood can be determined from the chemical plant's own risk assessment and the prevailing wind directions

How to determine the risk:

- Two types of fire:
  1. Internal (fire source is within the premises)
  2. External (e.g. wildfire or fire in adjacent buildings)
- In case 1 an internal risk assessment has to be performed
- In case 2 regional/local authorities can provide the risk indications for wildfires. The risk of adjacent building fire needs to be discussed with adjacent building owner.
- In the risk assessment, the risk of smoke or toxic fumes from an adjacent fire have to be taken into account as well.



## 8 CRI-008 – SECURITY INCIDENT

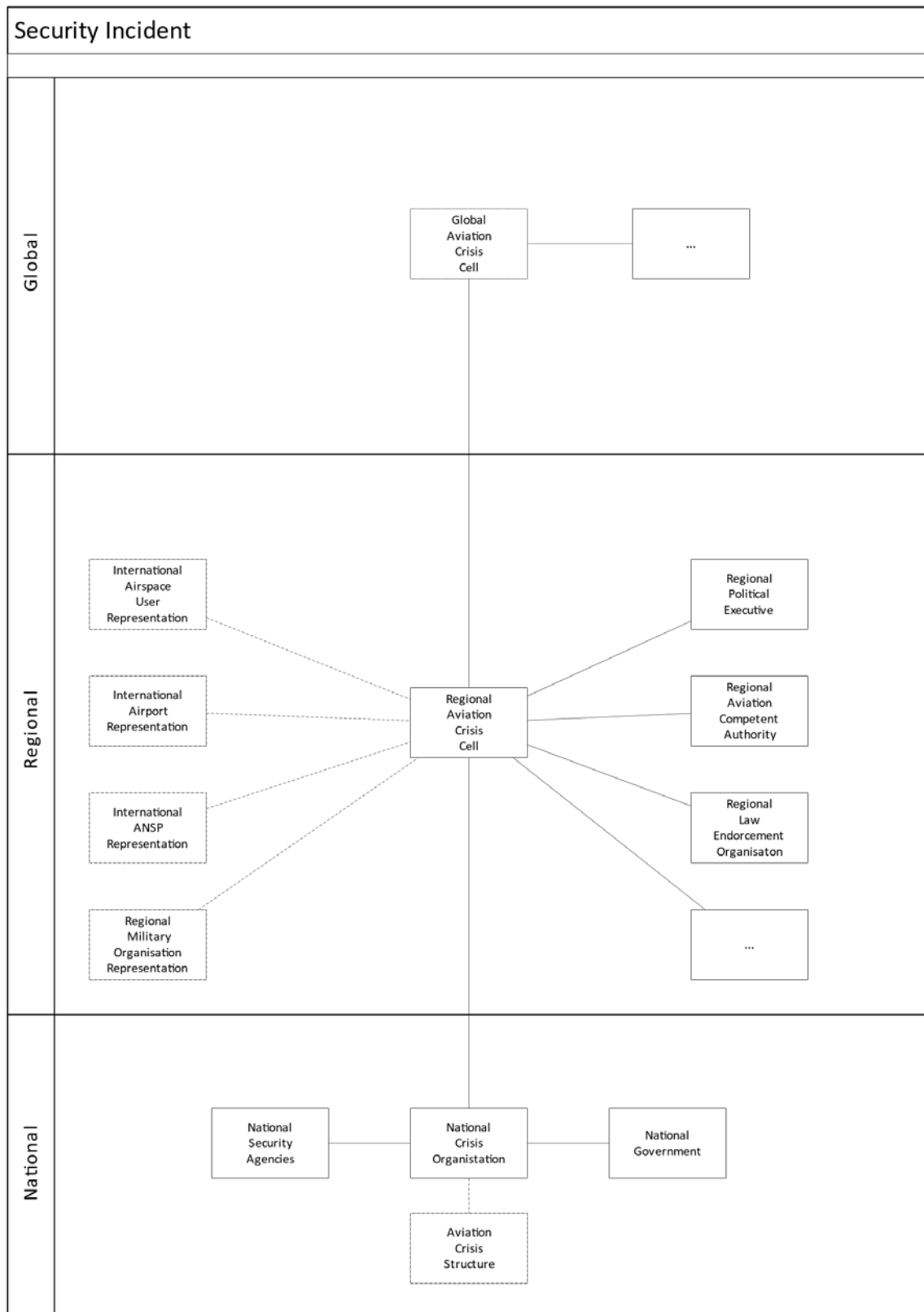
Security incidents in this context are defined as the threat of or actual physical attacks that lead to limitations in the availability of aviation infrastructure. This limitation can come from the attack itself or from (precautionary) security measures. In most cases the scope is national, but if regional infrastructure or multiple national infrastructures are affected, the impact may be regional.

How to determine the risk:

- The security risk landscape is very dynamic and diverse
- Regularly consult national/regional/local security authorities
- Scan the local threat horizon (e.g. environmental activists)

How to mitigate the risk:

- The security risk landscape is very dynamic and diverse
  - A variety of mitigation actions have to be applied (defence in depth):
    - Physical protection (e.g. perimeter defence, fortified buildings)
    - Monitoring (CCTV, guard inspections)
    - Staff vetting
    - Security procedures (minimal authority)



## 9 CRI-009 – AIRBORNE SPREAD OF DISEASES-PANDEMIC

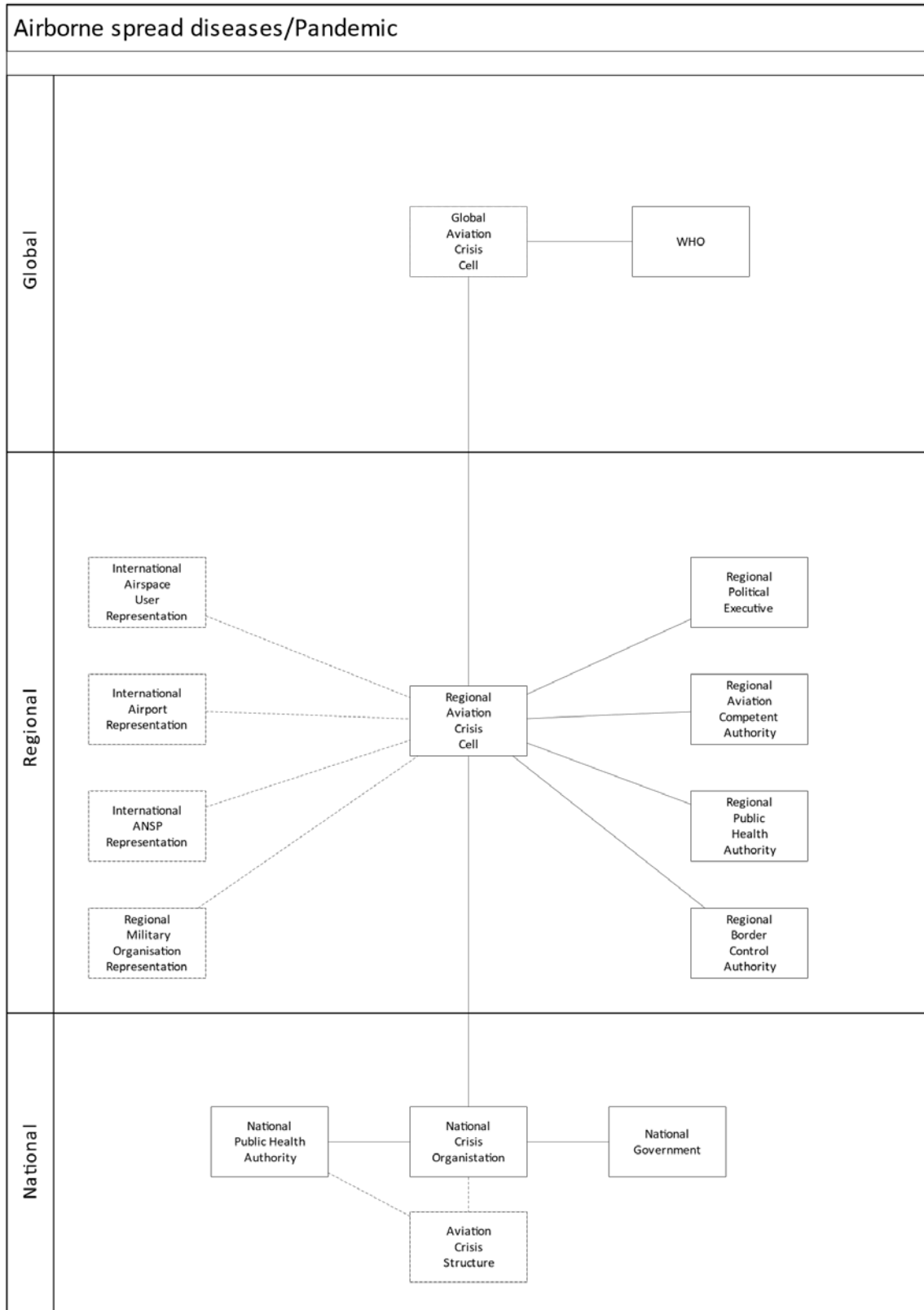
Airborne spread of severe infectious diseases will almost certainly lead to a global impact on aviation. It does not necessarily have impact on the availability of infrastructures, and COVID-19 showed that the impact on aviation was partly caused by public health decisions.

How to determine the risk:

- The risk is dynamic, not all elements can be assessed in a generic way
- Consult national/regional health authorities when a threat is pending
- Determine the exposure likelihood for local staff (and especially travelling staff)
- Determine the impact of reduced staff availability short and medium term

How to mitigate the risk:

- The risk is dynamic, mitigation may have to be tailored due to the type of pandemic/epidemic
- The following steps can be generically taken:
  - Procedures for hygiene at the site
  - Vaccination programs
  - Access limitations to site during sickness
  - Travel limitations to affected geographical areas



## 10 CRI-010 – MAJOR FAILURE OF PAN-EUROPEAN FUNCTION

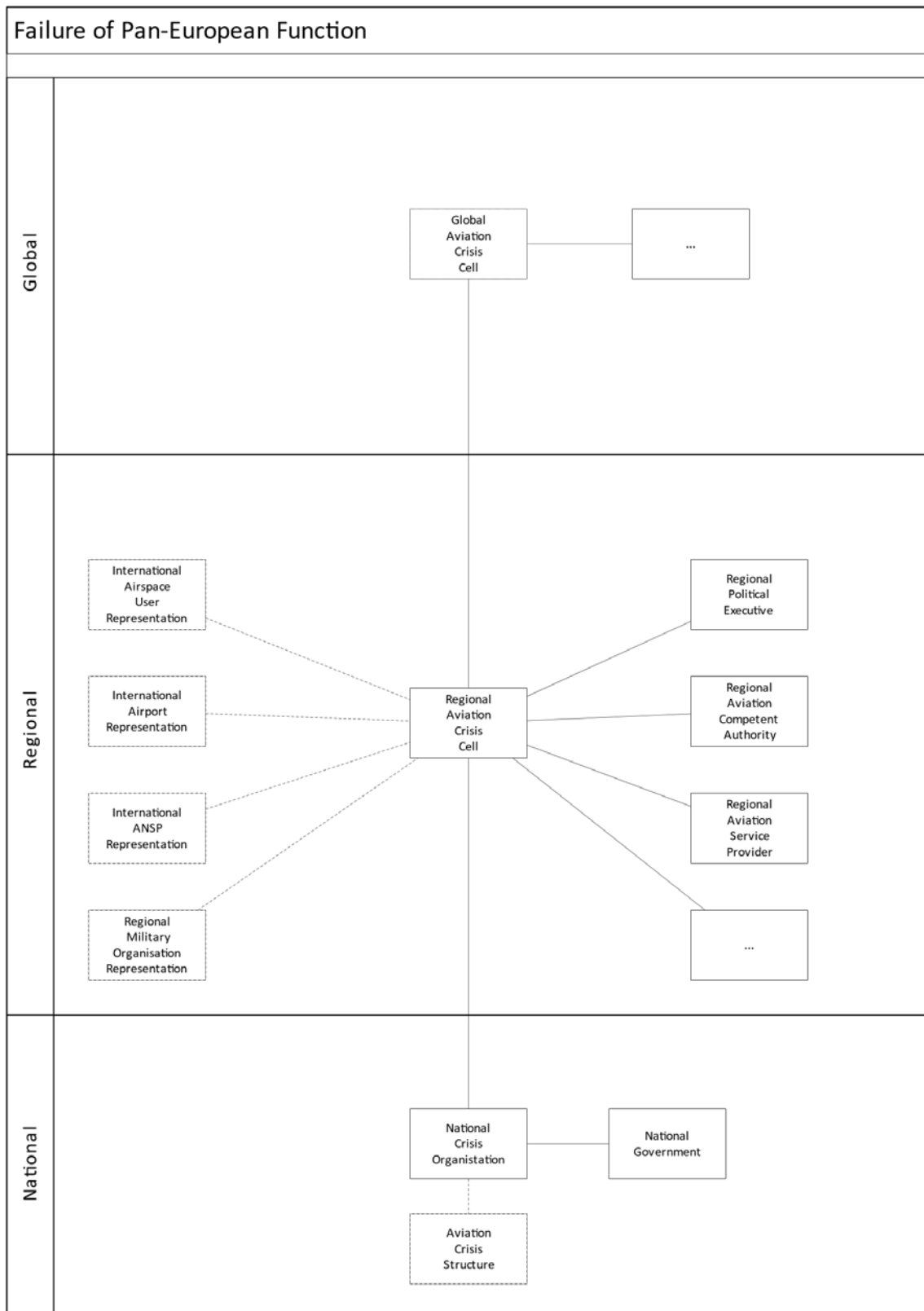
Aviation is increasingly relying on centralized functions. Several critical aviation functions have been regionally concentrated. The unavailability of such functions would immediately lead to regional (and potentially global) effects on aviation.

How to determine the risk:

- Similar to assessment of own infrastructure
- In case of SLAs, determine the feasibility of claims
- Keep good records of SLA adherence

How to mitigate the risk:

- Limit the dependency on pan-European functions
- Create local backup functions





## 11 CRI-011 – INDUSTRIAL ACTIONS

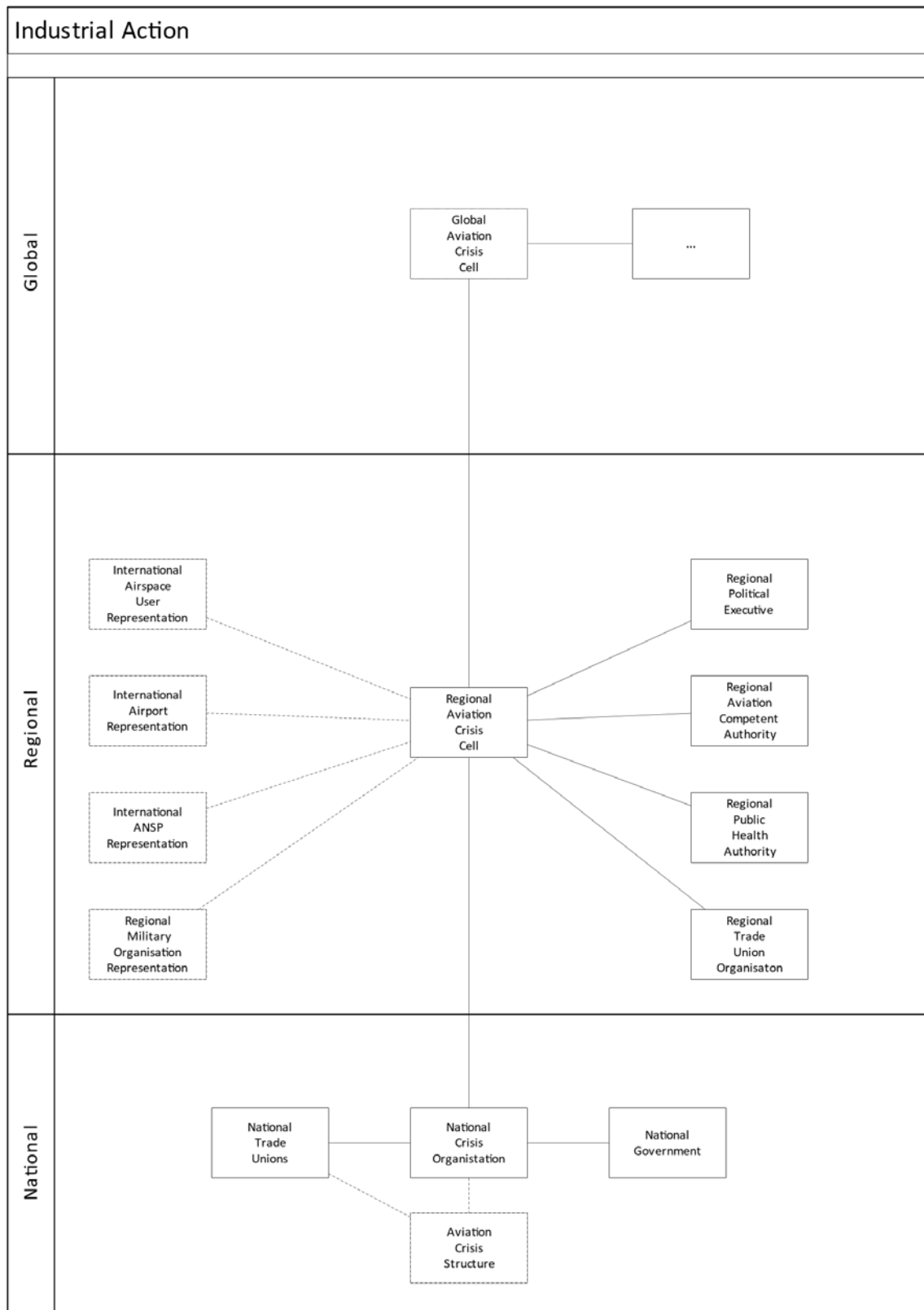
The majority of industrial actions have a (sub) national scope. Depending on the scale and type of service affected, the impact may be regional. Coordinated industrial actions across multiple states will certainly cause regional disruptions.

How to determine the risks:

- Identify potential dispute topics
- Develop scenarios for different outcomes of the social dialogue
- Analyse the impact of each scenario

How to mitigate the risk:

- Try to reach an agreement before the situation escalates
- Develop alternative scenarios with adjacent states



## 12 CRI-012 – CYBER ATTACK

The frequency of cyber-attacks, also in aviation, has been increasing for years and it is not likely that this will change in the foreseeable future. Compared to physical attacks, cyber-attacks can easily be expanded over large regions and even globally. Therefore, it can be expected to see cyber attacks on national, regional, and global level, where the likelihood decreases from national to global level.

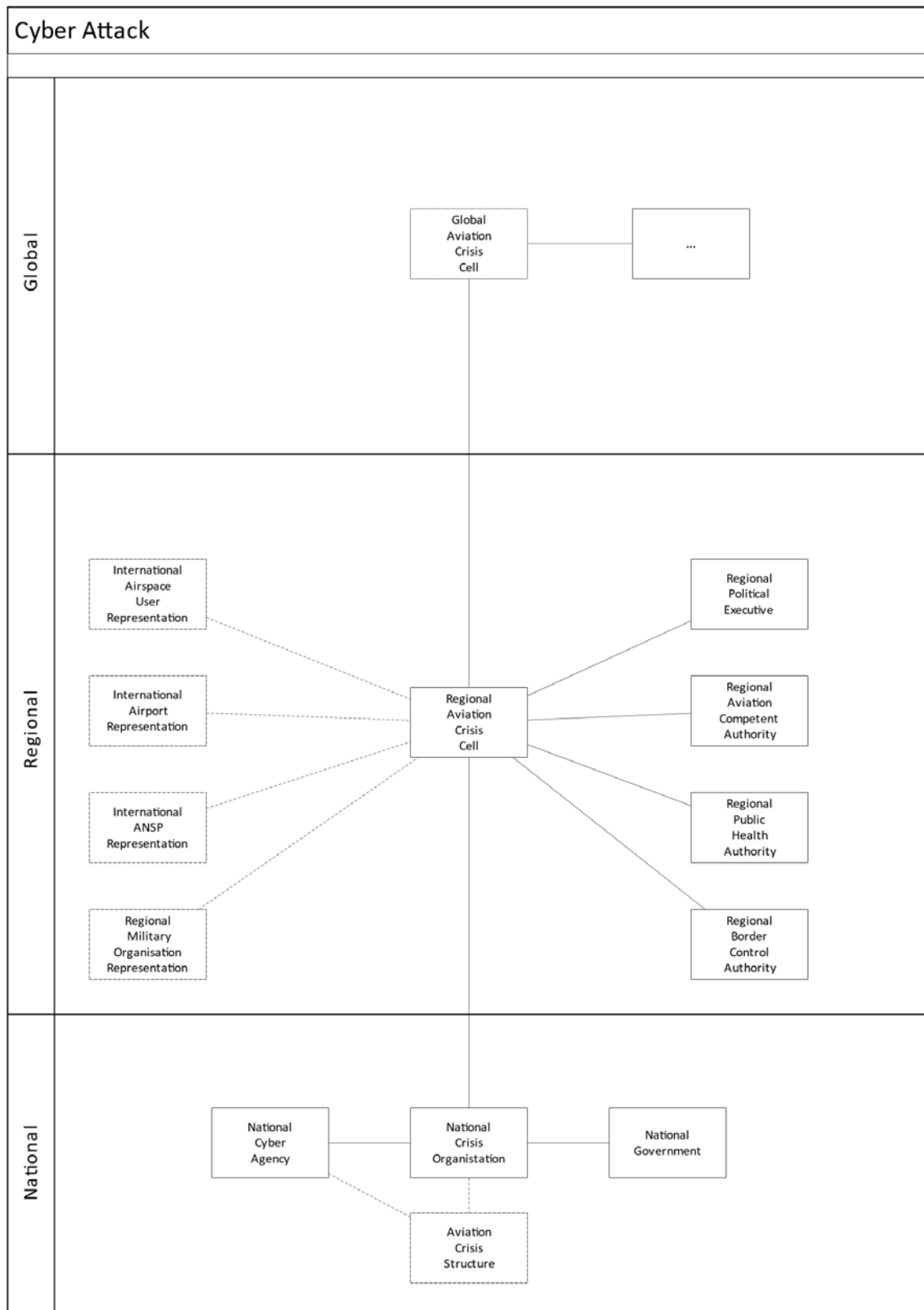
The impact that a cyber attack has depends on the service that is under attack and the impact the attack has on this service. The impact depends on the attack techniques used.

How to determine the risk:

- This is an external risk so—again—the likelihood of an attack cannot be influenced
- Consult the national (cyber)security authorities for information about threats
- Investigate vulnerabilities in processes and equipment
- Perform impact assessments for different threat scenarios
- In the risk determination, the fact that adjacent centres may have a similar problem has to be taken into account

How to mitigate the risk:

- This is an external risk so—again—the likelihood of an attack cannot be influenced
- Create awareness
- Train staff to recognise and be able to handle attacks
- Create a system architecture based on “defence in depth” principles
  - Layering
  - Diversity in systems
- Continuous (security specific) monitoring
- Create and practice backup and restore procedures



## 13 CRI-013 – SEVERE METEO SITUATION

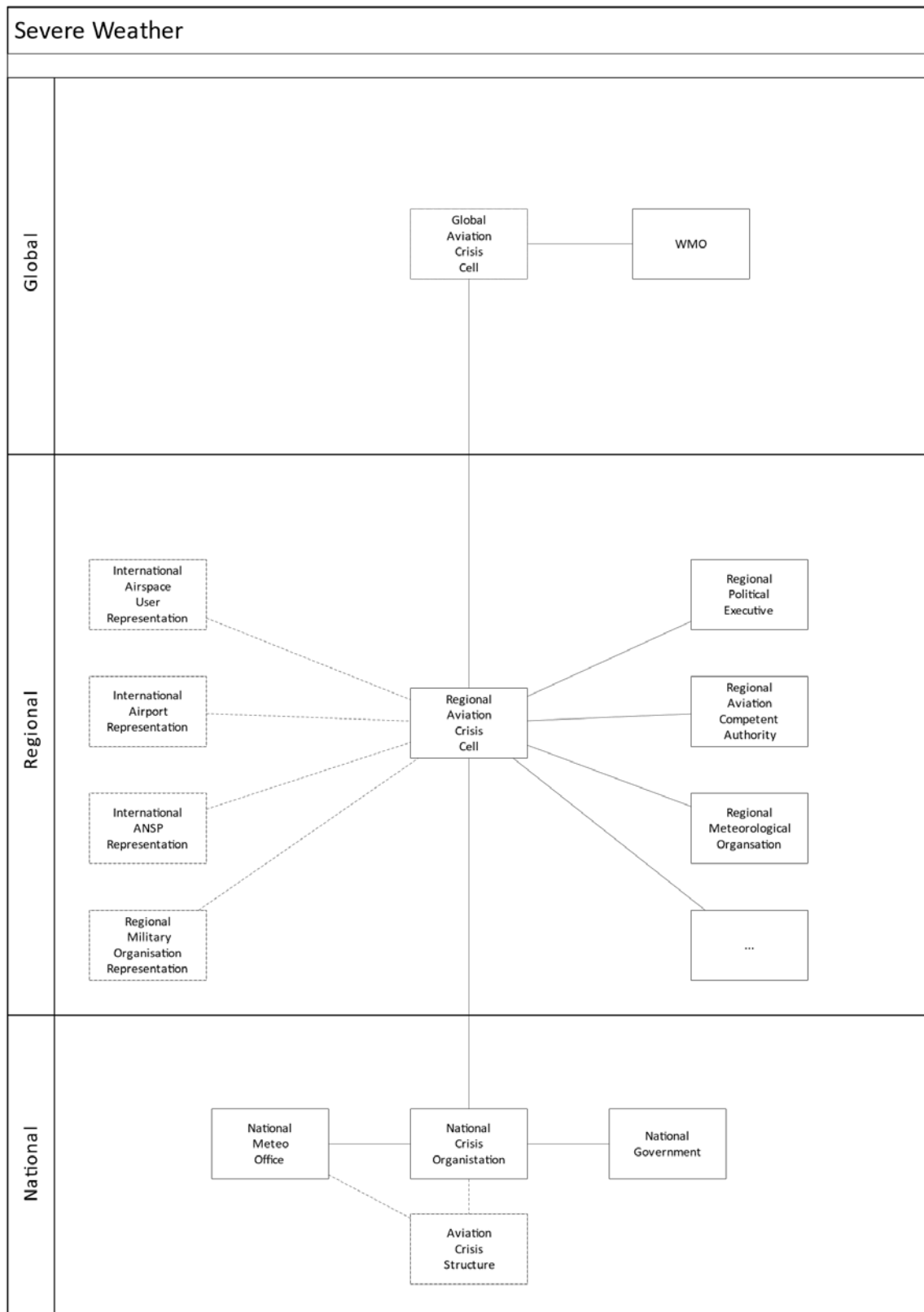
Although aviation has a long and successful history of dealing with severe weather conditions, the increasing traffic density and the effects of the global climate change may have increase the probability of weather based disruptions. Aviation relevant weather phenomena are of national (local thunderstorms, severe snowfall) or regional scope (large convective weather systems, storm depressions).

How to determine the risk:

- Weather related risk is quite diverse:
  - Operational aviation impact
  - Damage to own infrastructure (e.g., by storm, lightning)
  - Damage to external infrastructure (roads, power supply, communications services)
  - Accessibility of site (e.g., excessive snow, flooding of access roads)
- Consult the national weather service for weather related risks for the specific location
- Monitor the severe weather forecasts

How to mitigate the risk:

- Design the infrastructure to be able to withstand the worst expected weather.
  - Keep in mind to project future changes into the design process
- Ensure independence from potentially damaged infrastructure
  - At least have independent backup facilities
- Prepare and practice contingency procedures for heavy weather situations



## 14 CRI-014 – SPACE DEBRIS & METEORITES

Meteorites have been present since the beginning of the Earth. Despite the fact that thousands enter the Earth's atmosphere and presumably dozens reach the Earth's surface, evenly distributed across the globe. Since no confirmed collisions between meteorites and aircraft have been recorded, the probability can be considered to be low. In addition to this, the re-entry of meteorites is completely unpredictable, so no precautions can be taken.

Space debris in form of (un)controlled re-entries is also not a new phenomenon. The frequency of space debris fragments reaching the earth is on average in the same order of magnitude as for meteorites. Also in case of space debris, there are no confirmed collisions on record.

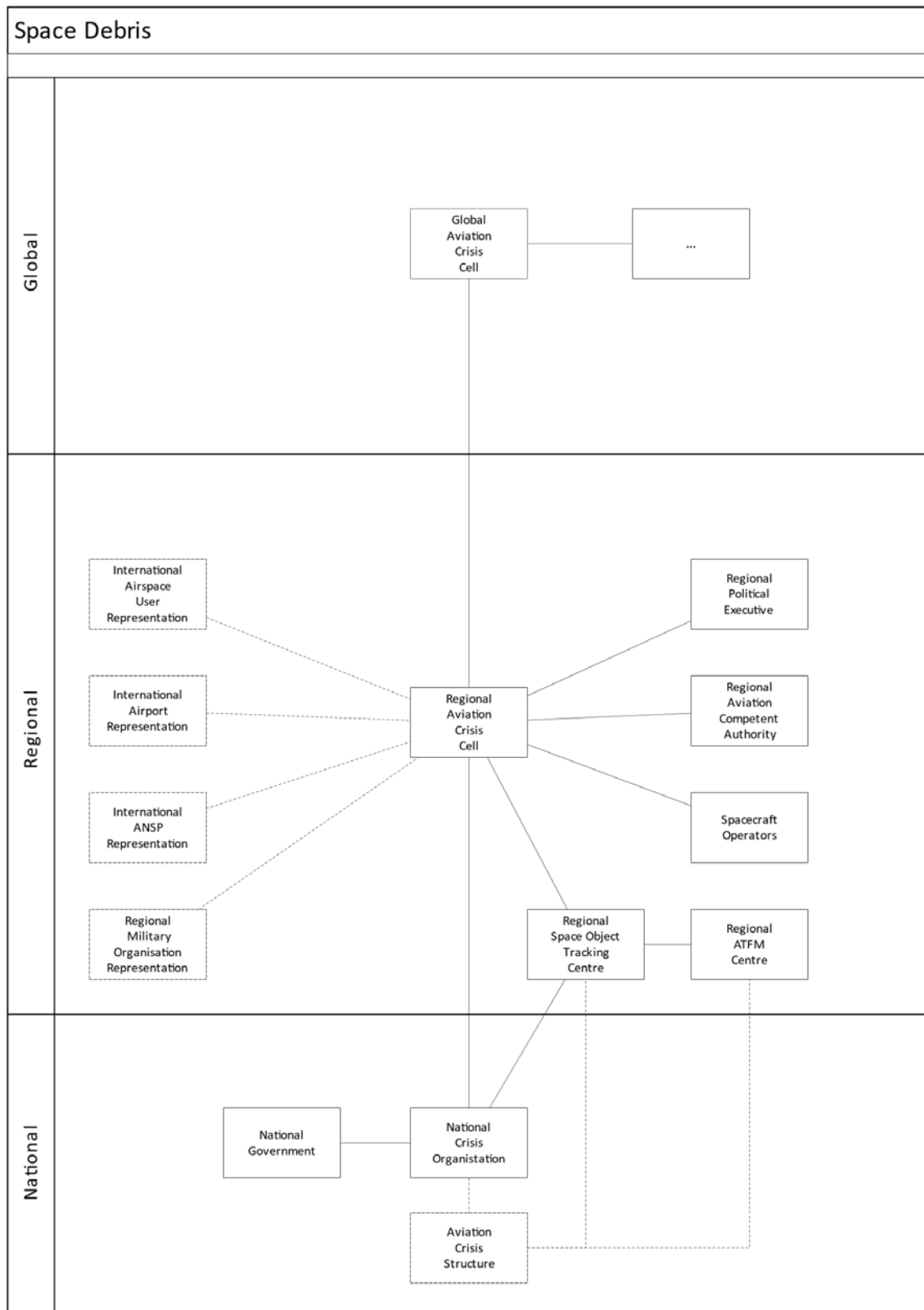
The main difference between meteorites and space debris is that the latter re-enters in a relatively small area, creating a debris cloud with a fragment density that is significantly higher than the meteorite density. Therefore, a risk analysis should be undertaken in case of a known re-entry.

How to determine the risk:

- In general, the space debris risk is very low and does not require a general analysis
- In case of imminent exposure, the collision risk should be discussed with agencies like ESA or NASA

How to mitigate the risk:

- In case of imminent exposure the collision risk should be discussed with agencies like ESA or NASA





## 15 CRI-015 – SPACE WEATHER

Aviation relevant space weather events, usually, are the result of solar activity. The solar activity increases and decreases following an 11-year cycle. Although severe solar events can occur at any time, the probability increases towards the maximum of the cycle.

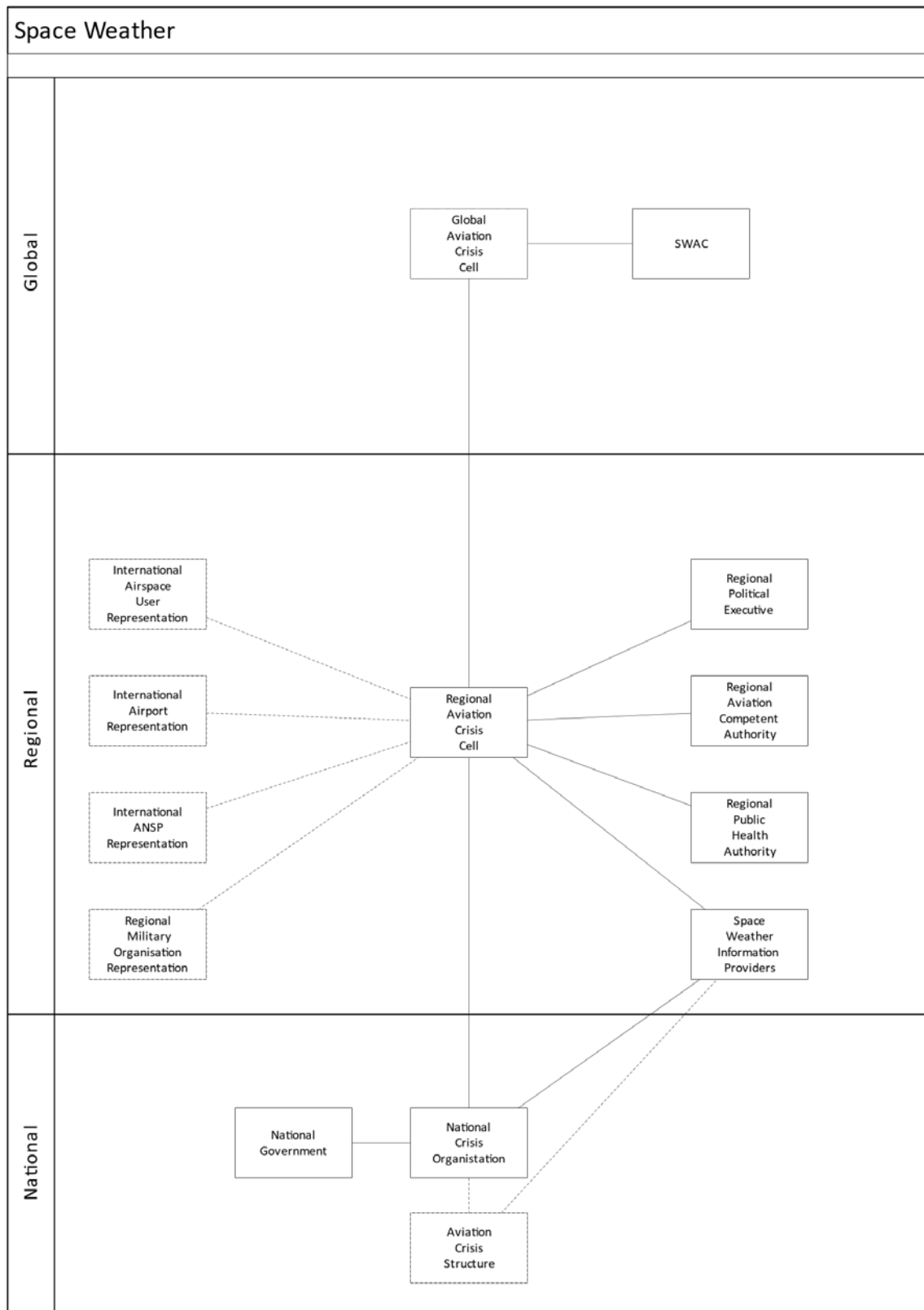
Space weather events can directly affect the crew and passengers as well as airborne and space-based electronics, through radiation exposure.

How to determine the risk:

- Analyse the susceptibility of systems to space weather
  - External communication links
  - Surveillance sensors
  - External services (e.g., GNSS, satellite ADS-(B/C), communications satellites)
- Monitor the space weather situation

How to mitigate the risk:

- Reduce the susceptibility of systems to space weather
  - Shielding
  - Diversity
  - Using optical wide area communications wherever possible
- Take technical and operational precautions in case of space weather alert



## 16 CRI-016 – SHORTAGE OF FUEL

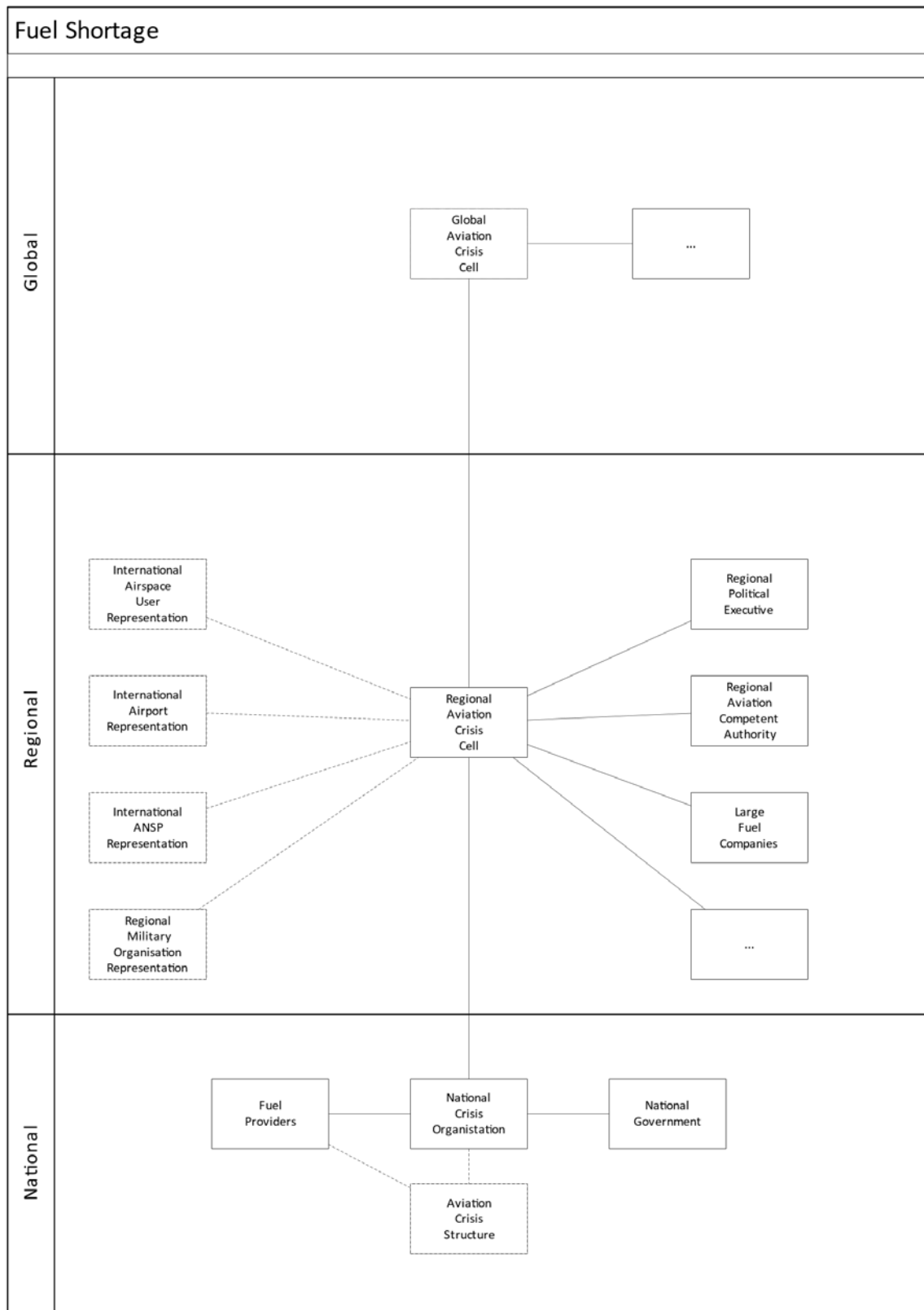
Shortage of (jet) fuel can be the result of production problems and logistic problems. The most likely cause for production problems would be the availability of crude oil. The refinery capacity is well spread over a lot of countries. More likely that production problems are logistics problems either due do blocking of pipelines or shipping routes (regional impact) or due to national problems in the distribution chain (e.g. industrial action). Oil has been seen as a political instrument in the past 50 years, therefore this component needs to be considered in the risk assessment.

How to determine the risk:

- Analyse the supply chain and identify the potential “weak spots”
- Monitor the global political situation

How to mitigate the risk

- Eliminate the weak spots in the supply chain
- Create buffers



## 17 CRI-017 – LARGE SCALE POWER OUTAGE

Large (multinational) scale power outages will have a large impact on society. Since the majority of aviation stakeholders is equipped with backup power systems, they will not be directly affected by the outage.

There are important secondary effects of the power outage that will have a severe impact on aviation operations. The most immediate will be the outage of communication services. The local communication nodes typically have backup power for several hours.

The scale of the events and the related uncertainty will also affect the appetite of passengers to fly.

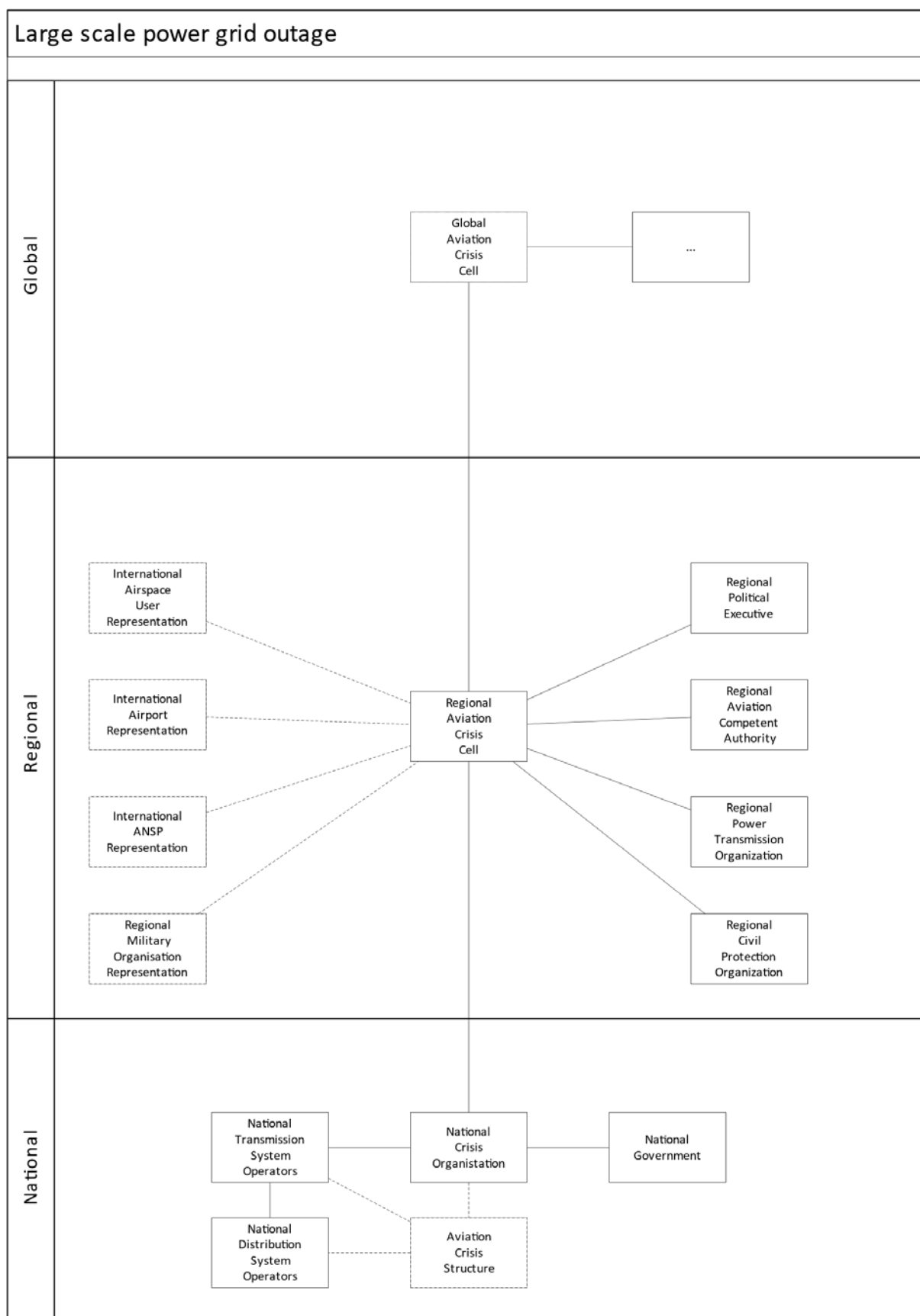
Large scale outages can last for hours to days and very large outages could take weeks to fully recover.

How to determine the risk:

- Review the local backup capacity
- Investigate dependencies and their backup capacities

How to mitigate risk:

- Ensure that the backup facilities ready for operations
- Discuss minimum “survivability” requirements with service providers



## 18 CRI-018 – LARGE SCALE COMMUNICATION NETWORK OUTAGE

Large scale communication network outages are the scenarios that have potentially the largest impact on aviation. Due to its nature, the impact will almost be immediate and unlike electrical power, local mitigations are not possible, since communication requires the sender, the receiver and all the elements in between need to work.

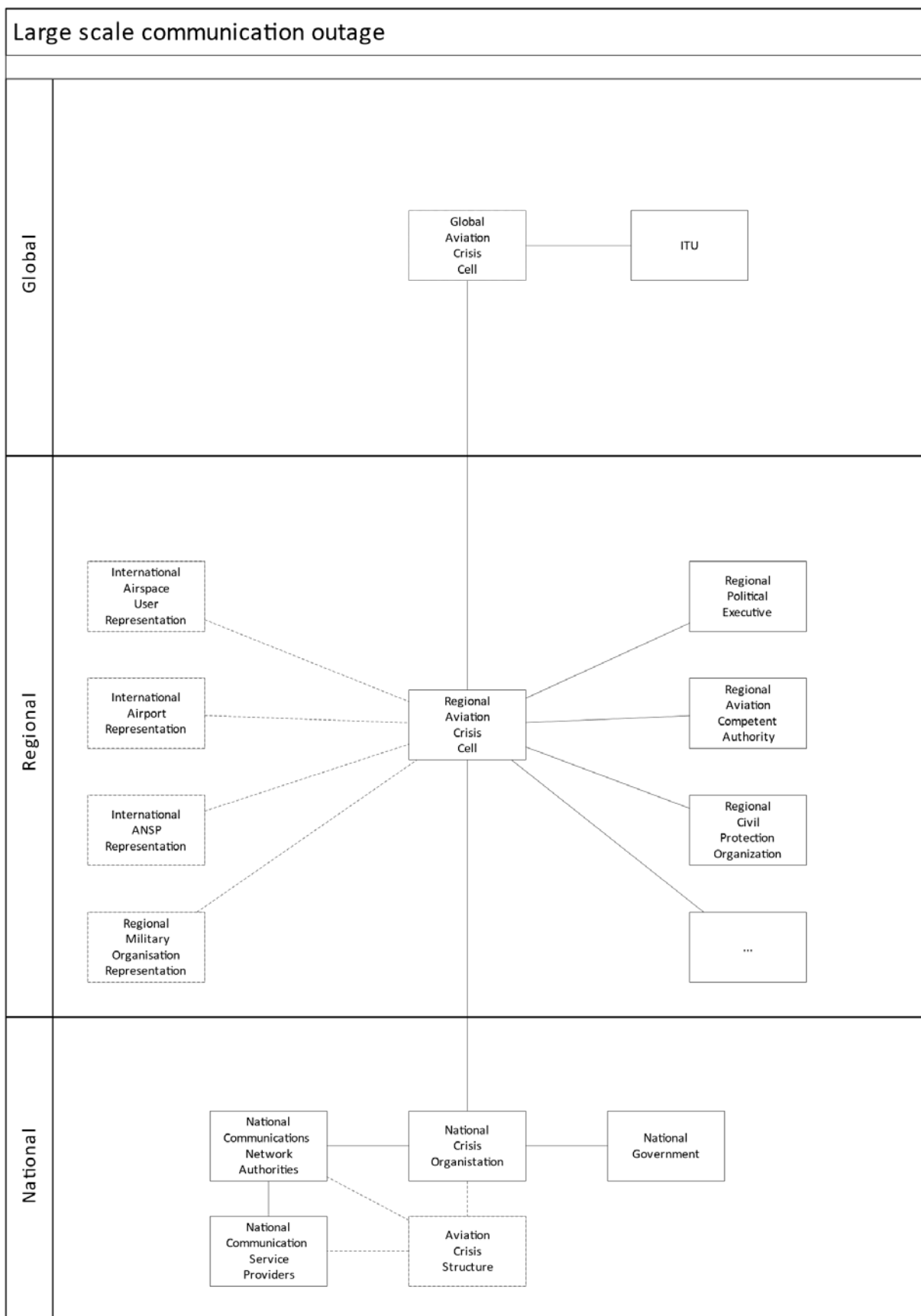
A further complicating factor is that recovery may take longer, since the recovery effort cannot be effectively coordinated due to the absence of communication means.

How to determine the risk:

- Determine the dependencies on communication networks
- Investigate the robustness of the communication infrastructure in use

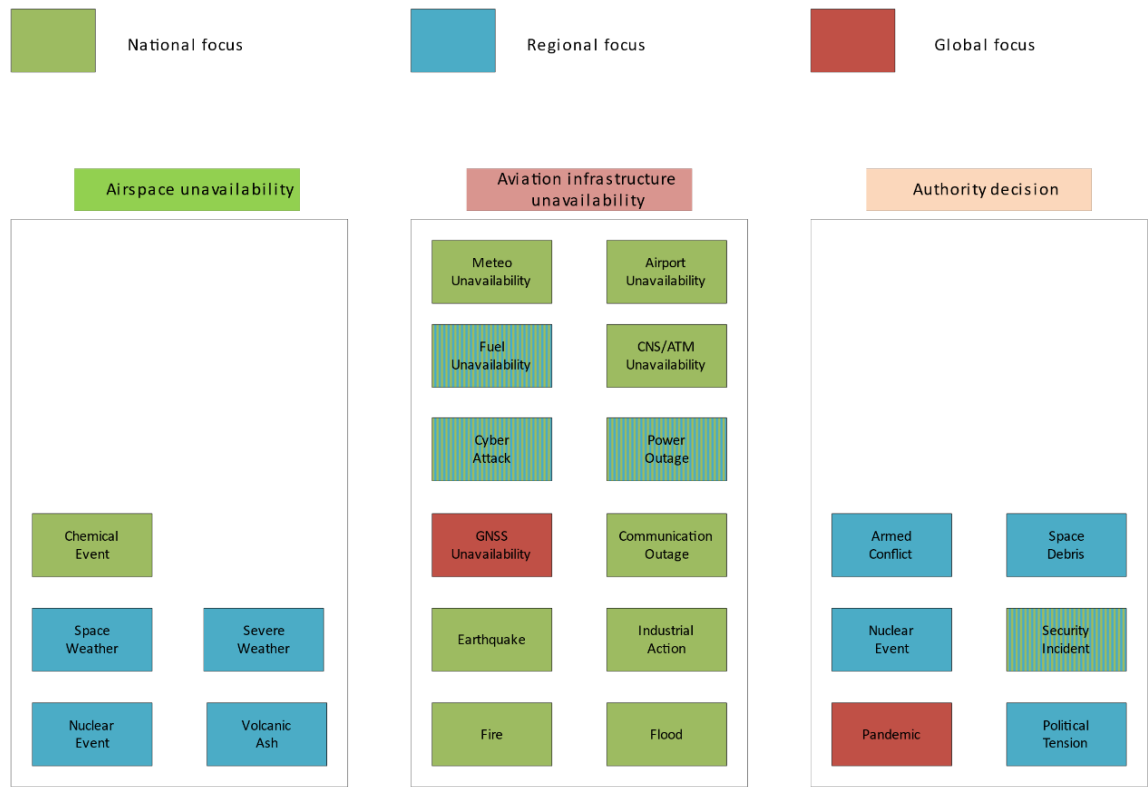
How to mitigate the risk:

- Avoid unnecessary dependencies
- Ensure sufficient redundancy and diversity in the communication infrastructure
- Implement last resorts (for recovery coordination)



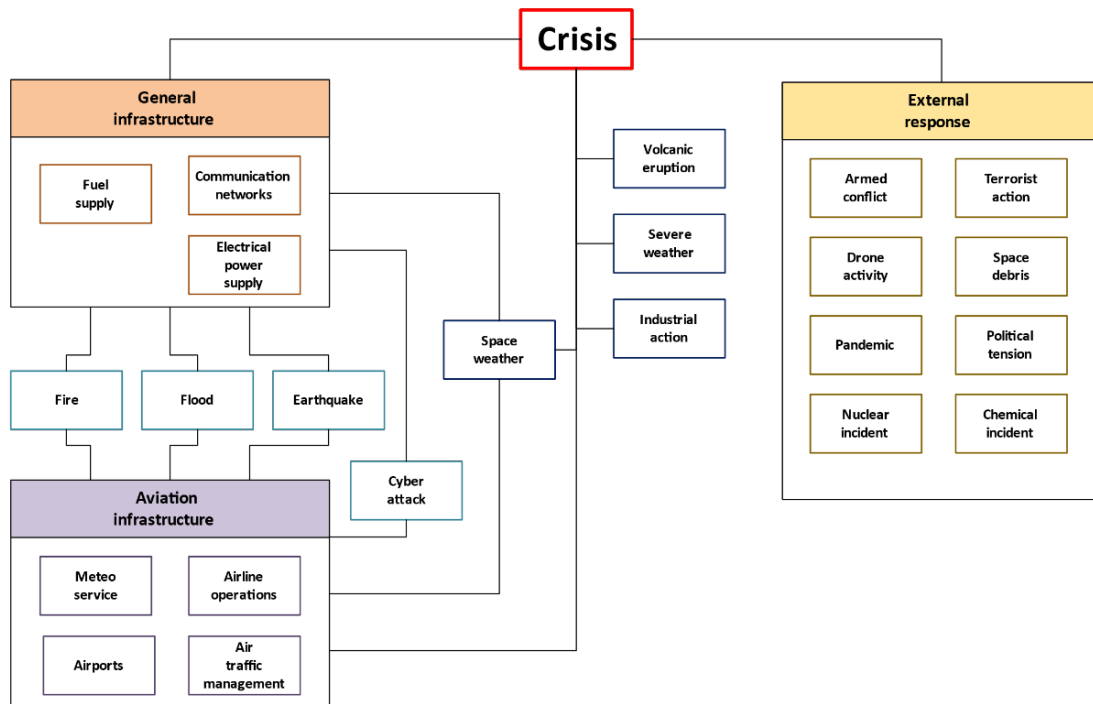


APPENDIX B – SCENARIO SCOPE<sup>8</sup>



<sup>8</sup> It should be noted that the response by authorities may lead to airspace unavailability.

## APPENDIX C – SCENARIO RELATIONSHIPS



## APPENDIX D – RISK REGISTER EXAMPLE

1. Table 3 shows an example of a risk register entry. It contains the relevant information about the risk of a scenario and a log of changes including rationale.
2. Table 4 contains a graph that shows an overview of the scenarios including their respective risks

**Table 3: Example of risk register entry**




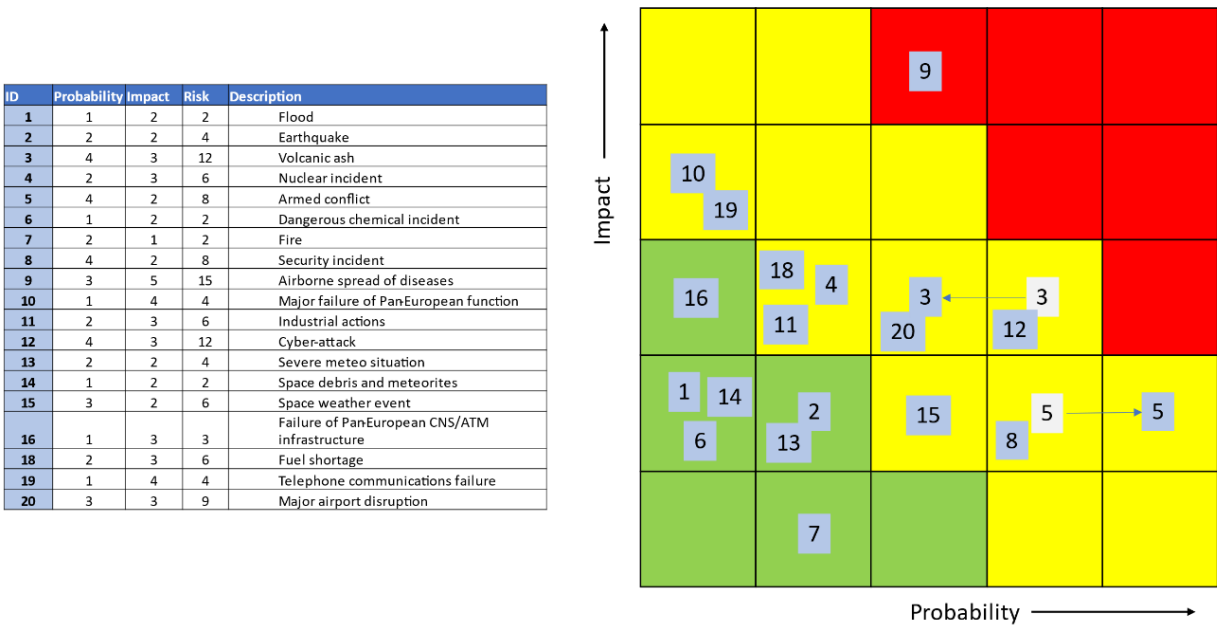
| ID                                                                                                                                                                                                                                                                                                                                        |     | Scenario name                                        |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----|------------------------------------------------------|-----|--------------------------------------------------------------------|-------|---------------------|------------------------------------------------------------------------------------|----------------|-------------------------------------------------------------------------------------|--------------|-------------------------------------------------------------------------------------|
| CRI-012                                                                                                                                                                                                                                                                                                                                   |     | Cyber-Attack                                         |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Scenario description                                                                                                                                                                                                                                                                                                                      |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| A large scale cyber-attack with compromise of information, compromise of functions or infrastructure and loss of essential services resulting in denial of air navigation service; attack on any infrastructure on aircraft, airport, ANSP and infrastructure, directly as well as indirectly, i.e. access, power supplies, telecom, etc. |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Impact range                                                                                                                                                                                                                                                                                                                              |     | Probability range                                    |     | Base risk range                                                    |       | Current probability |                                                                                    | Current impact |                                                                                     | Current risk |                                                                                     |
| Min                                                                                                                                                                                                                                                                                                                                       | Max | Min                                                  | Max | Max                                                                | Min   | 4.0                 |  | 3.0            |  | 12.00        |  |
| 1.0                                                                                                                                                                                                                                                                                                                                       | 5.0 | 3.0                                                  | 5.0 | 3.00                                                               | 25.00 |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Geographical scale                                                                                                                                                                                                                                                                                                                        |     | Duration                                             |     | Type of crisis                                                     |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Min                                                                                                                                                                                                                                                                                                                                       | Max | Min                                                  | Max | Potential unavailability of general and/or aviation infrastructure |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| 1.0                                                                                                                                                                                                                                                                                                                                       | 4.0 | 1.0                                                  | 2.0 |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Rationale for risk assessment                                                                                                                                                                                                                                                                                                             |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Impact on aircraft (immediate): aircraft equipment impacted.                                                                                                                                                                                                                                                                              |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Impact on airspace: Airspace unavailable for flight ops; reduced capacity.                                                                                                                                                                                                                                                                |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Impact on aerodrome: Aerodrome unavailable for flight ops; reduced capacity; infrastructure (building, equipment, access).                                                                                                                                                                                                                |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Impact on flight operations: Flight cancellation/ re-routeing/ re-scheduling/ diversion/ delay.                                                                                                                                                                                                                                           |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Impact on ANSP: People (ATCOs workload); infrastructure (building, equipment, access); communications.                                                                                                                                                                                                                                    |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Impact on persons: Crew workload/ health; passenger health/ handling; ground personnel workload.                                                                                                                                                                                                                                          |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Impact on cargo: Livestock; goods (including dangerous goods).                                                                                                                                                                                                                                                                            |     |                                                      |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Date                                                                                                                                                                                                                                                                                                                                      |     | Rationale for risk adjustment                        |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| 25-11-2022                                                                                                                                                                                                                                                                                                                                |     | Trend adjustment. The cyberattack risk remains high. |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              |                                                                                     |
| Date                                                                                                                                                                                                                                                                                                                                      |     | Log entry                                            |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              | By                                                                                  |
| 25-11-2022                                                                                                                                                                                                                                                                                                                                |     | Updated risk trend                                   |     |                                                                    |       |                     |                                                                                    |                |                                                                                     |              | HDH                                                                                 |

Table 4: Risk register overview graph



— END —